

COLUMBIA GAS OF PENNSYLVANIA, INC.
53.52

Applicability; public utilities other than canal, turnpike, tunnel, bridge and wharf companies.

- (a) Whenever a public utility, other than a canal, turnpike, tunnel, bridge or wharf company files a tariff, revision or supplement effecting changes in the terms and conditions of service rendered or to be rendered, it shall submit to the Commission, with the tariff, revision or supplement, statements showing all of the following:

- (1) The specific reasons for each change.

Response (Kempic):

The rate changes are being proposed to allow Columbia Gas of Pennsylvania a reasonable opportunity to recover revenue sufficient to cover its operating expenses and increases to rate base and provide a reasonable opportunity to earn a fair rate of return.

- (2) The total number of customers served by the utility.

Response (Kempic): Refer to Exhibit No. 3.

- (3) A calculation of the number of customers, by tariff subdivisions, whose bills will be affected by the change.

Response (Johnson): Refer to Exhibit No.103, Schedule No. 8.

- (4) The effect of the change on the utility's customers.

Response (Johnson): Refer to Exhibit No. 103, Schedule No. 8.

- (5) The direct or indirect effect of the proposed change on the utility's revenue and expenses.

Response (Kempic): Refer to Exhibit Nos. 3 and 4.

COLUMBIA GAS OF PENNSYLVANIA, INC.
53.52

- (6) The effect of the change on the service rendered by the utility.

Response (Kempic): Service rendered by the utility will not be impacted by the changes to rates.

- (7) A list of factors considered by the utility in its determination to make the change. The list shall include a comprehensive statement about why these factors were chosen and the relative importance of each. This subsection does not apply to a portion of a tariff change seeking a general rate increase as defined in 66 Pa. C.S. §1308 (relating to voluntary changes in rates).

Response (Kempic): Not Applicable.

- (8) Studies undertaken by the utility in order to draft its proposed change. This paragraph does not apply to a portion of a tariff change seeking a general rate increase as defined in 66 Pa. C.S. §1308.

Response (Kempic): Not Applicable.

- (9) Customer polls taken and other documents which indicate customer acceptance and desire for the proposed change. If the poll or other documents reveal discernible public opposition, an explanation of why the change is in the public interest shall be provided

Response (Kempic): No customer polls were taken to indicate customer acceptance and desire for the proposed rate changes.

COLUMBIA GAS OF PENNSYLVANIA, INC.

53.52

- (10) Plans the utility has for introducing or implementing the changes with respect to its ratepayers.

Response (Kempic): Columbia will notify its ratepayers of the proposed changes through a bill insert in compliance with the Commission's Regulations (Pa Code Section 53.45).

- (11) F.C.C., F.E.R.C. or Commission orders or rulings applicable to the filing.

Response (Kempic): There are no orders or rulings that directly apply to this change.

- (b) Whenever a public utility, other than a canal, turnpike, tunnel, bridge or wharf company files a tariff, revision, or supplement which will increase or decrease the bills to its customers, it shall submit in addition to the requirements of subsection (a), to the Commission, with the tariff, revision or supplement, statements showing all of the following:

- (1) The specific reason for each increase or decrease.

Response (Kempic): The rate changes are being proposed to allow Columbia Gas of Pennsylvania a reasonable opportunity to recover revenue sufficient to cover its operating expenses and increases to rate base and provide a reasonable opportunity to earn a fair rate of return.

COLUMBIA GAS OF PENNSYLVANIA, INC.
53.52

- (2) The operating income statement of the utility for a 12-month period, the end of which may not be more than 120 days prior to the filing.

Response (Kempic): Refer to Exhibit No.2.

- (3) A calculation of the number of customers, by tariff subdivision, whose bills will be increased.

Response (Johnson): Refer to Exhibit No. 103, Schedule No. 8.

- (4) A calculation of the total increase, in dollars, by tariff subdivision, projected to an annual basis.

Response (Johnson): Refer to Exhibit No. 103, Schedule No. 8.

- (5) A calculation of the number of customers, by tariff subdivision, whose bills will be decreased.

Response (Johnson): Refer to Exhibit No.103, Schedule No. 8.

- (6) A calculation of the total decreases, in dollars, by tariff subdivision, projected to an annual basis.

Response (Johnson): Refer to Exhibit No.103, Schedule No. 8.

COLUMBIA GAS OF PENNSYLVANIA, INC
53.53 II RATE OF RETURN
A. ALL UTILITIES

13. Attach copies of the summaries of the projected two years' Company's budgets (revenues, expense, and capital).

Response:

Please see the Company's response to Standard Data Request GAS-ROR-13 for projected revenues and expenses.

Please see the Company's response to Standard Data Request GAS-ROR-14 for the projected construction budget.

Columbia Gas of Pennsylvania, Inc.
Docket No. R-2024-3046519
Referenced by Commission Regulations

Commission Regulation Number	Commission Regulation	Historic Test Year Twelve Months Ended November 30, 2023		Fully Projected Future Test Year Twelve Months Ended December 31, 2025		Witness
		Exhibit	Schedule	Exhibit	Schedule	
53.52	<u>Applicability: Public Utilities Other Than Canal, Turnpike, Bridge, and Wharf Companies</u>					
53.52(a)	Whenever a public utility, other than a canal, turnpike, tunnel, bridge or wharf company files a tariff, revision or supplement effecting changes in the terms and conditions of service rendered or to be rendered, it shall submit to the Commission, with the tariff, revision, or supplement, statements showing all of the following:	13	3			Kempic
53.52(a)1	The specific reasons for each change.	13	1	113	1	Kempic/Johnson
53.52(a)2	The total number of customers served by the utility.	3 13	1	103 113	1	Battig Kempic
53.52(a)3	A calculation of the number of customers, by tariff subdivision, whose bills will be affected by the change.	3 13	1	103 113	1	Battig Kempic
53.52(a)4	The effect of the change on the utility's customers.	3 13	1	103 113	1	Battig Kempic
53.52(a)5	The direct or indirect effect of the proposed change on the utility's revenue and expenses.	13	1	113	1	Kempic/Johnson
53.52(a)6	The effect of the change on the service rendered by the utility	13	1	113	1	Kempic/Johnson
53.52(a)7	A list of factors considered by the utility in its determination to make the change. The list shall include a comprehensive statement about why these factors were chosen and the relative importance of each. This subsection does not apply to a portion of a change seeking a general rate increase as defined in 66 Pa. C. S. & 1308 (relating to voluntary changes in rates).	13	1	113	1	Kempic/Johnson
53.52(a)8	Studies undertaken by the utility in order to draft its proposed change. This paragraph does not apply to a portion of a tariff change seeking a general rate increase as defined in 66 Pa. C. S. & 1308.	13	1	113	1	Kempic/Johnson
53.52(a)9	Customer polls taken and other documents which indicate customer acceptance and desire for the proposed change. If the poll or other documents reveal discernible public opposition, an explanation of why the change is in the public interest shall be provided.	13	1	113	1	Kempic/Johnson
53.52(a)10	Plans the utility has for introducing or implementing the changes with respect to its ratepayers.	13	1	113	1	Kempic/Johnson
53.52(a)11	FCC. FERC or Commission orders or rulings applicable to the filing.	13	1	113	1	Kempic/Johnson
53.52(b)	Whenever a public utility, other than a canal, turnpike, tunnel, bridge or wharf company files a tariff, revision or supplement which will increase or decrease the bills to its customers, it shall submit in addition to the requirements of subsection (a), to the Commission, with the Tariff, revision, or supplement, statements showing all of the following:	13	3			Kempic/Johnson

Columbia Gas of Pennsylvania, Inc.
Docket No. R-2024-3046519
Referenced by Commission Regulations

Commission Regulation Number	Commission Regulation	Historic Test Year Twelve Months Ended <u>November 30, 2023</u>		Fully Projected Future Test Year Twelve Months Ended <u>December 31, 2025</u>		Witness
		<u>Exhibit</u>	<u>Schedule</u>	<u>Exhibit</u>	<u>Schedule</u>	
53.52(b)1	The specific reasons for each Increase or decrease.	13	1	113	1	Kempic/Johnson
53.52(b)2	The operating income statement of the utility for a 12-month period, the end of which may not be more than 120 days prior to the filing.	2 3 13	1	102 103 113	1 1	Komenda Battig Kempic
53.52(b)3	A calculation of the number of customers, by tariff subdivision, whose bills will be increased.	3 13	1	103 113	1	Battig Kempic
53.52(b)4	A calculation of the total increases, in dollars, by tariff subdivision, projected to an annual basis.	3 13	1	103 113	1	Battig Kempic
53.52(b)5	A calculation of the number of customers, by tariff subdivision, whose bills will be decreased.	3 13	1	103 113	1	Battig Kempic
53.52(b)6	A calculation of the total decreases, in dollars, by tariff subdivision, projected to an annual basis.	3 13	1	103 113	1	Battig Kempic
53.52(c)1	A Statement showing the utility's calculation of the rate of return earned in the 12-month period referred to on subsection (b)(2), and the anticipated rate of return to be earned when the tariff, revision, or supplemental becomes effective. The rate base used in this calculation shall be supported by summaries of original cost for the rate of return calculation.	8		108		Covert
53.52(c)2	A detailed balance sheet of the utility as of the close of the period referred to in subsection (b)f2).	1	1	101		Komenda
53.52(c)3	A summary, by detailed plant accounts, of the book value of the property of the utility at the date of the balance sheet required by paragraph (2).	8	1, 2	108		Covert
53.52(c)4	A statement showing the amount of the depreciation reserve, at the date of the balance sheet required by paragraph (2), applicable to the property, summarized as required by paragraph (3).	8	3	108	3	Covert
53.52(c) 5	A statement of operating income, setting forth the operating revenues and expenses by detailed accounts for the 12-month period ending on the balance sheet required by paragraph (2).	2	1	102	1	Komenda
53.52(c) 6	A brief description of a major change in the operating or financial condition of the utility occurring between the date of the balance sheet required by paragraph (2) and the date of transmittal of the tariff, revision or supplement. As used on this paragraph, a major change is one which materially alters the operating or financial condition of the utility from that reflected in paragraphs (1) - (5).	1	2	101		Komenda
<u>53.53 I A</u>	<u>53.53 I. VALUATION</u> <u>A. ALL UTILITIES</u>					
53.53.I.A.1	Provide a corporate history (include the dates of original incorporation, subsequent mergers and/or acquisitions). Indicate all countries and cities and other governmental subdivisions to which service is provided (including service areas outside the state), and the total population in the area served.	15	1	115		Danhires

Columbia Gas of Pennsylvania, Inc.
Docket No. R-2024-3046519
Referenced by Commission Regulations

Commission Regulation Number	Commission Regulation	Historic Test Year Twelve Months Ended <u>November 30, 2023</u>		Fully Projected Future Test Year Twelve Months Ended <u>December 31, 2025</u>		Witness
		<u>Exhibit</u>	<u>Schedule</u>	<u>Exhibit</u>	<u>Schedule</u>	
53.53.I.A.2	Provide a schedule showing the measures of value and the rates of return at the original cost and trended original cost measures of value at the spot, three-year and five-year average price levels. All claims made on this exhibit should be cross-referenced to appropriate exhibits. Provide a schedule similar to the one listed above, reflecting respondent's final claim in its previous rate case.	8		108		Covert
53.53.I.A.3	Provide a description of the depreciation methods utilized in calculating annual depreciation amounts and depreciation reserves, together with a discussion of all factors which were considered in arriving at estimates of service life and dispersion by account. Provide dates of all field inspections and facilities visited.	9	1	109	1	Spanos
53.53.I.A.4	Set forth, in exhibit form, charts depicting the original and estimated survivor curves and a tabular presentation of the original life table plotted on the chart for each account where the retirement rate method of analysis is utilized. a. If any utility plant was excluded from the measures of value because it was deemed not to be "used and useful" in the public service, supply a detailed description of each item of property. b. Provide the surviving original cost at test year end by vintage by account and include applicable depreciation reserves and annuities. (i) These calculations should be provided for plant in service as well as other categories of plant, including, but not limited, to contributions in aid of construction, customer's advances for construction, and anticipated retirements associated with any construction work in progress claims (if Applicable)	9	1	109	1	Spanos
53.53.I.A.5	Provide a comparison of respondent's calculated depreciation reserve vs. book reserve by account at the end of the test year.	9	2	109	2	Spanos
53.53.I.A.6	Supply a schedule by account and depreciable group showing the survivor curve and annual accrual rate estimated to be appropriate: a. For the purposes of this filing. b. For the purposes of the most recent rate increase filing prior to the current proceedings. (i) Supply a comprehensive statement of any changes made in method of depreciation and in the selection of average service lives and dispersion.	9	3	109	3	Spanos
53.53.I.A.7	Provide a table, showing the cumulative depreciated original cost by year of installation for utility plant in service at the end of the test year (depreciable plant only) as claimed in the measures of value, in the following form: a. Year installed. b. Original cost - the total surviving cost associated with each installation year from all plant accounts.	9	4	109	4	Spanos

Columbia Gas of Pennsylvania, Inc.
Docket No. R-2024-3046519
Referenced by Commission Regulations

Commission Regulation Number	Commission Regulation	Historic Test Year Twelve Months Ended <u>November 30, 2023</u>		Fully Projected Future Test Year Twelve Months Ended <u>December 31, 2025</u>		Witness
		<u>Exhibit</u>	<u>Schedule</u>	<u>Exhibit</u>	<u>Schedule</u>	
	c. Calculated depreciation reserve-the calculated depreciation reserve associated with each installation year from all plant accounts. d. Depreciated original cost - (Column B minus Column C). e. Total - cumulation year by year of the figures from Column D. f. Column E divided by the total of the figure in Column D.	9	4	109	4	Spanos
53.53.I.A.8	Provide a description of the trending methodology which was utilized. Identify all indexes which were used (include all backup workpapers) and all the reasons particular indexes were chosen. If indexes were spliced, indicate which years were utilized in any splices. if indexes were composite, show all supporting calculations, include any analysis made to "test" the applicability of any index.	8		108		Covert
53.53.I.A.9	Provide an exhibit indicating the spot trended original cost at test year end by vintage by account and include applicable depreciation reserves. Include total by account for all other trended measures of value.	8		108		Covert
53.53.I.A.10	Supply an exhibit indicating the percentages of Undepreciated original cost which were trended with the following indexes: a. Boeckh. b. Handy-Whitman. c. Indexes developed from suppliers' prices. d. Indexes developed from company records and company price histories. e. Construction equipment. f. Government statistical releases.	8		108		Covert
53.53.I.A.11	Provide a table, showing the cumulative trended depreciated original cost (at the spot price level) by year installation for utility plant in service at the end of the test year (depreciable plant only) as claimed in the measures of value, in the following form: a. Year installed. b. Trended original cost (at the spot price level) - the total surviving cost associated with each installation year from all plant accounts. c. Trended calculated depreciation reserve - the calculated depreciation reserve associated with each installation year from all plant accounts. d. Depreciated trended original cost - (Column B minus Column C). e. Total-accumulation year by year of the figures from Column D. f. Column E divided by the total of the figures in Column D.	8		108		Covert
53.53.I.A.12	If a claim is made for construction work in progress, include, in the form of an exhibit, the summary page from all work orders, amount expensed at the end of the test year and anticipated in-service dates. Indicate if any of the construction work in progress will result in insurance recoveries, reimbursements, or retirements of existing facilities. Describe in exact detail the necessity of each project claimed if not detailed on the summary page from the work order. Include final completion date and estimated total amounts to be spent on each project. [These exhibits should be updated at the conclusion of these proceedings.]	8		108		Covert

Columbia Gas of Pennsylvania, Inc.
Docket No. R-2024-3046519
Referenced by Commission Regulations

Commission Regulation Number	Commission Regulation	Historic Test Year Twelve Months Ended <u>November 30, 2023</u>		Fully Projected Future Test Year Twelve Months Ended <u>December 31, 2025</u>		Witness
		<u>Exhibit</u>	<u>Schedule</u>	<u>Exhibit</u>	<u>Schedule</u>	
53.53.I.A.13	If a claim is made for non-revenue producing construction work in progress, include, in the form of an exhibit, the summary page from all work orders, amount expensed at the end of the test year and anticipated in-service dates. Indicate if any of the construction work in progress will result in insurance recoveries, reimbursements, or retirements of existing facilities. Describe in exact detail the necessity of each project claimed if not detailed on the summary page from the work order. Include final completion date and estimated total amounts to be spent on each project. [These exhibits should be updated at the conclusion of these proceedings.]	8		108		Covert
53.53.I.A.14	If a claim is made for plant held for future use, supply the following: a. A brief description of the plant or land site and its cost. b. Expected date of use for each item claimed. c. Explanation as to why it is necessary to acquire each item in advance of its date of use. d. Date when each item was acquired. e. Date when each item was placed in plant held for future use.	8		108		Covert
53.53.I.A.15	If materials and supplies comprise part of the cash working capital claim, attach an exhibit showing the actual book balances for materials and supplies by month for the thirteen months prior to the end of the test year. Explain any abrupt changes in monthly balances. [Explain method of determining claim if other than that described above.]	8		108		Covert
53.53.I.A.16	If fuel stocks comprise part of the cash working capital claim, provide an exhibit showing the actual book balances (quantity and price) for the fuel inventories by type of fuel for the thirteen months prior to the end of the test year by location, station, etc. [Explain the method of determining claim if other than that described above.]	8		108		Covert
53.53.I.A.17	Regardless of whether a claim for net negative or positive salvage is made, attach an exhibit showing gross salvage, cost of removal, and net salvage for the test year and four previous years by account.	9	5	109	5	Spanos
53.53.I.A.18	Explain in detail by statement or exhibit the appropriateness of claiming any additional items, not previously mentioned, in the measures of value.	8		108		Covert
<u>53.53.I.C</u>	<u>53.53.I VALUATION</u> <u>C. GAS UTILITIES</u>					
53.53.I.C.1	Provide, with respect to the scope of operations of the utility, a description of all property, including an explanation of the system's operation, and all plans for any significant future expansion, modification, or other alterations of facilities. This description should include, but not be limited to the following: a. If respondent has various gas service areas, indicate if they are integrated, such that the gas supply is available to all customers. b. Provide all pertinent data regarding company policy related to the addition of new consumers in the company's service area. c. Explain how respondent obtains its gas supply, as follows: (i) Explain how respondent stores or manufactures gas; if applicable. (ii) State whether the company has peak shaving facilities. (iii) Provide details of coal-gasification programs, if any. iv) Describe the potential for emergency purchases of gas. (v) Provide the amount of gas in MCF supplied by various suppliers in the test year (include a copy of all contracts).	17		117		Battig

Columbia Gas of Pennsylvania, Inc.
Docket No. R-2024-3046519
Referenced by Commission Regulations

Commission Regulation Number	Commission Regulation	Historic Test Year Twelve Months Ended <u>November 30, 2023</u>		Fully Projected Future Test Year Twelve Months Ended <u>December 31, 2025</u>		Witness
		<u>Exhibit</u>	<u>Schedule</u>	<u>Exhibit</u>	<u>Schedule</u>	
	d. Provide plans for future gas supply, as follows: (i) Supply details of anticipated gas supply from respondent's near-term development of gas wells, if any. (ii) Provide gas supply agreements and well development ventures and identify the parties thereto. e. Indicate any anticipated curtailments and explain the reasons for the curtailments. f. Provide current data on any Federal Power Commission action or programs that may affect, or tend to affect, the natural gas supply to the gas utility.	17		117		Battig
53.53.I.C.2	Provide an overall system map, including and labeling all measuring and regulating stations, storage facilities, production facilities transmission and distribution mains, by size, and all interconnections with other utilities and pipelines.	15	2	115		Danhires
<u>53.53.II.A</u>	<u>53.53.II. RATE RETURN</u> <u>A. ALL UTILITIES</u>					
53.53.II.A.1	Provide capitalization and capitalization ratios for the last five-year period and projected through the next two years. (With short-term debt and without short-term debt.) Company, Parent and System (consolidated)). a. Provide year-end interest coverages before and after taxes for the last three years and at latest date. (Indenture and SEC Bases.) (Company, Parent and System (consolidated)). b. Provide year-end preferred stock dividend coverages for last three years and at latest date (Charter and SEC bases).	401		401		Moul
53.53.II.A.2	Provide latest quarterly financial report (Company and Parent).	402		402		Moul
53.53.II.A.3	Provide latest Stockholder's Report (Company and Parent).	403		403		Moul
53.53.II.A.4	Provide latest Prospectus (Company and Parent).	404		404		Moul
53.53.II.A.5	Supply projected capital requirements and sources of Company, Parent and System (consolidated) for each of future three years.	405		405		Moul
53.53.II.A.6	Provide a schedule of debt and preferred stock of Company, Parent and System (Consolidated) as of test year-end and latest date, detailing for each issue (if applicable): a. Date of issue b. Date of maturity c. Amount issued d. Amount outstanding e. Amount retired f. Amount reacquired g. Gain on reacquisition h. Coupon rate i. Discount or premium at issuance j. Issuance expenses k. Net proceeds l. Sinking Fund requirements m. Effective interest rate n. Dividend rate o. Effective cost rate p. Total average weighted effective Cost Rate	406		406		Moul

Columbia Gas of Pennsylvania, Inc.
Docket No. R-2024-3046519
Referenced by Commission Regulations

Commission Regulation Number	Commission Regulation	Historic Test Year Twelve Months Ended <u>November 30, 2023</u>		Fully Projected Future Test Year Twelve Months Ended <u>December 31, 2025</u>		Witness
		<u>Exhibit</u>	<u>Schedule</u>	<u>Exhibit</u>	<u>Schedule</u>	
53.53.II.A.7	Supply financial data of Company and/or Parent for last five years: a. Earnings-price ratio (average) b. Earnings-book value ratio (per share basis) (avg. book value) c. Dividend yield (average) d. Earnings per share (dollars) e. Dividends per share (dollars) f. Average book value per share yearly g. Average yearly market price per share (monthly high-low basis) h. Pre-tax funded debt interest coverage i. Post-tax funded debt interest coverage j. Market price-book value ratio	407		407		Moul
53.53.II.A.8	State amount of debt interest utilized for income tax calculations, and details of debt interest computations, under each of the following rate cases vases: a. Actual test year b. Annualized test year-end c. Proposed test year-end	7		107		Harding
53.53.II.A.9	State amount of debt interest utilized for income tax calculations which has been allocated from the debt interest of an affiliate, and details of the allocation, under each of the following rate cases vases: a. Actual test year b. Annualized test year-end c. Proposed test year-end	7		107		Harding
53.53.II.A.10	Under Section 1552 of the Internal Revenue Code and Regulations 1.1552-1 thereunder, if applicable, Parent Company, in filing a consolidated income tax return for the group, must choose one of four options by which it must allocate total income tax liability of the group to the participating members to determine each member's tax liability to the federal government. (If this interrogatory is not applicable, so state.) a. State what option has been chosen by the group. b. Provide, in summary form, the amount of tax liability that has been allocated to each of the participating members in the consolidated income tax return c. Provide a schedule, in summary form, of contributions, which were determined on the basis of separate tax return calculations, made by each of the participating members to the tax liability indicated in the consolidated group tax return. Provide total amounts of actual payments to the tax depository for the tax year, as computed on the basis of separate returns of members. d. Provide annual income tax return for group, and if income tax return shows net operating loss, provide details of amount of net operating loss allocated to the income tax returns of each of the members of the consolidated group.	7		107		Harding

Columbia Gas of Pennsylvania, Inc.
Docket No. R-2024-3046519
Referenced by Commission Regulations

Commission Regulation Number	Commission Regulation	Historic Test Year Twelve Months Ended <u>November 30, 2023</u>		Fully Projected Future Test Year Twelve Months Ended <u>December 31, 2025</u>		Witness
		<u>Exhibit</u>	<u>Schedule</u>	<u>Exhibit</u>	<u>Schedule</u>	
53.53.II.A.11	Provide AFUDC charged by company at test year-end and latest date, and explain method by which rate was calculated.	408		408		Covert
53.53.II.A.12	Set forth provisions of Company's and Parent's charter and indentures (if applicable) which describe coverage requirements, limits on proportions of types of capital outstanding, and restrictions on dividend payouts.	409		409		Moul
53.53.II.A.13	Attach copies of the summaries of the projected 2 year's Company's budgets (revenue, expense and capital).	13	2	113	2	Komenda
53.53.II.A.14	Describe long-term debt reacquisition's by Company and Parent as follows: a. Reacquisition's by issue by year. b. Total gain on reacquisition's by issue by year. c. Accounting of gain for income tax and book purposes.	410		410		Moul
53.53.II.A.15	Set forth amount of compensating bank balances required under each of the following rate base bases: a. Annualized test year operations. b. Operations under proposed rates.	411		411		Moul
53.53.II.A.16	Provide the following information concerning compensating bank balance requirements for actual test year: a. Name of each bank. b. Address of each bank. c. Types of accounts with each bank (checking, savings, escrow, other services, etc.). d. Average Daily Balance in each account. e. Amount and percentage requirements for compensating bank balance at each bank. f. Average daily compensating bank balance at each bank. g. Documents from each bank explaining compensating bank balance requirements. h. Interest earned on each type of account.	411		411		Moul
53.53.II.A.17	Provide the following information concerning bank notes payable for actual test year: a. Line of Credit at each bank. b. Average daily balances of notes payable to each bank, by name of bank. c. interest rate charged on each bank note (Prime rate, formula rate or other). d. Purpose of each bank note (e.g., construction, fuel storage, working capital, debt retirement). e. Prospective future need for this type of financing	412		412		Moul
53.53.II.A.18	Set forth amount of total cash (all cash accounts) on hand from balance sheets for last 24-calendar months preceding test year-end.	1	3	101		Komenda
53.53.II.A.19	Submit details on Company or Parent common stock offerings (past 5 years to present) as follows: a. Date of Prospectus b. Date of offering c. Record date d. Offering period-dates and number of days e. Amount and number of share of offering	413		413		Moul

Columbia Gas of Pennsylvania, Inc.
Docket No. R-2024-3046519
Referenced by Commission Regulations

Commission Regulation Number	Commission Regulation	Historic Test Year Twelve Months Ended November 30, 2023		Fully Projected Future Test Year Twelve Months Ended December 31, 2025		Witness
		Exhibit	Schedule	Exhibit	Schedule	
	f. Offering ratio (if rights offering) g. Per cent subscribed h. Offering price i. Gross proceeds per share j. Expenses per share j. Net proceeds per share (i-j) l. Market price per share 1. At record date 2. At offering date 3. One month after close of offering m. Average market price during offering 1. Price per share 2. Rights per share-average value of rights n. Latest reported earnings per share at time of offering o. Latest reported dividends at time of offering	413		413		Moul
53.53.II.A.20	Provide latest available balance sheet and income statement for Company, Parent and System (consolidated).	414		414		Komenda
53.53.II.A.21	Provide Original Cost, Trended Original Cost and Fair Value rate base claims.	8		108		Covert
53.53.II.A.22	a. Provide Operating Income claims under: (i) Present rates (ii) Pro forma present rates (annualized & normalized) (iii) Proposed rates (annualized & normalized) b. Provide Rate of Return on Original Cost and Fair Value claims under: (i) Present rates (ii) Pro forma present rates (iii) Proposed rates	2	2	102	2	Komenda
53.53.II.A.23	List details and sources of "Other Property and Investments," "Temporary Cash Investments and Working Funds on test year-end balance sheet.	1	4	101		Komenda
53.53.II.A.24	Attach chart explaining Company's corporate relationship to its affiliates (System Structure).	15	3	115		Kempic
53.53.II.A.25	If the utility plans to make a formal claim for a specific allowable rate of return. Provide the following data in statement form: a. Claimed capitalization and capitalization ratios with supporting data. b. Claimed cost of long-term debt with supporting data. c. Claimed cost of short-term debt with supporting data. d. Claimed cost of total debt with supporting data. e. Claimed cost of preferred stock with supporting data f. Claimed cost of common equity with supporting data.	400		400		Moul
53.53.II.A.26	Provide the following income tax data: a. Consolidated income tax adjustments, if applicable. b. Interest for tax purposes (basis).	7		107		Harding
53.53.II.C	53.53.II. RATE RETURN C. GAS UTILITIES					
53.53.II.C.1	Provide test year monthly balances for "Current Gas Storage" and notes financing such storage.	1	5	101		Komenda

Columbia Gas of Pennsylvania, Inc.
Docket No. R-2024-3046519
Referenced by Commission Regulations

Commission Regulation Number	Commission Regulation	Historic Test Year Twelve Months Ended November 30, 2023		Fully Projected Future Test Year Twelve Months Ended December 31, 2025		Witness
		Exhibit	Schedule	Exhibit	Schedule	
53.53.III.A	53.53.III. BALANCE SHEET AND OPERATING STATEMENT A ALL UTILITIES					
53.53.III.A1	Provide a comparative balance sheet for the test year and the preceding year which corresponds with the test year date.	1	1	101		Komenda
53.53.III.A2	Set forth the major items of Other Physical Property, Investments in Affiliated Companies and Other Investments.	1	6	101		Komenda
53.53.III.A3	Supply the amounts and purpose of Special Cash Accounts of all types, such as: a. Interest and Dividend Special Deposits. b. Working Funds other than general operating cash accounts. c. Other special cash accounts and amounts (Temporary cash investments).	1	7	101		Komenda
53.53.III.A4	Describe the nature and/or origin and amounts of notes receivable, accounts receivable from associated companies, and any other sign fact receivables, other than customer accounts, which appear on balance sheet.	1	8	101		Komenda
53.53.III.A5	Provide the amount of accumulated reserve for uncollectible accounts, method and rate of accrual, amounts accrued, and amounts written-off in each of the last three years.	1	9	101		Komenda
53.53.III.A6	Provide a list of prepayments and give an explanation of special prepayments.	1	10	101		Komenda
53.53.III.A7	Explain in detail any other significant (in amount) current assets listed on balance sheet.	1	11	101		Komenda
53.53.III.A8	Explain in detail, including the amount and purpose, the deferred asset accounts that currently operate to effect or will at a later date effect the operating account supplying: a. Origin of these accounts. b. Probable changes to this account in the near future. c. Amortization of these accounts currently charged to operations or to be charged in the near future. d. Method of determining yearly amortization for the following accounts: Temporary Facilities Miscellaneous Deferred Debits Research and Development Property Losses Any other deferred accounts that effect operating results.	1	12	101		Komenda
53.53.III.A9	Explain the nature of accounts payable to associated companies, and note amounts of significant items.	1	13	101		Komenda
53.53.III.A10	Provide details of other deferred credits as to their origin and disposition policy (e.g. - amortization).	1	14	101		Komenda
53.53.III.A11	Supply basis for Injury and Damages reserve and amortization thereof.	1	15	101		Komenda
53.53.III.A12	Provide details of any significant reserves, other than depreciation, bad debt, injury and damages, appearing on balance sheet.	1	16	101		Komenda
53.53.III.A13	Provide an analysis of Unappropriated retained earnings for the test year and three preceding calendar years.	1	17	101		Komenda
53.53.III.A14	Provide schedules and data in support of the following working capital items: a. Prepayments - List and identify all items b. Federal Excise Tax accrued and prepaid c. Federal Income Tax accrued or prepaid d. Pa. State Income Tax accrued or prepaid e. Pa. Gross Receipts Tax accrued or prepaid	8		108		Covert

Columbia Gas of Pennsylvania, Inc.
Docket No. R-2024-3046519
Referenced by Commission Regulations

Commission Regulation Number	Commission Regulation	Historic Test Year Twelve Months Ended <u>November 30, 2023</u>		Fully Projected Future Test Year Twelve Months Ended <u>December 31, 2025</u>		Witness
		<u>Exhibit</u>	<u>Schedule</u>	<u>Exhibit</u>	<u>Schedule</u>	
	f. Pa. Capital Stock Tax accrued or prepaid g. Pa. Public Utility Realty Tax accrued or prepaid h. State sales tax accrued or prepaid i. Payroll taxes accrued or prepaid j. Any adjustment related to the above items for ratemaking purposes.	8		108		Covert
53.53.III.A15	Supply an exhibit supporting the claim for working capital requirement based on the lead-lag method. a. Pro forma expenses and revenues are to be used in lieu of book data for computing lead-lag days. b. Respondent must either include sales for resale and related expenses in revenues and in expenses or exclude from revenues and expenses. Explain procedures followed (exclude telephone).	8	4	108	4	Covert
53.53.III.A16	Provide detailed calculations showing the derivation of the tax liability offset against gross cash working capital requirements.	8	4	108	4	Covert
53.53.III.A17	Prepare a Statement of Income for the various time frames of the rate proceeding including: Col. 1-Book recorded statement for the test year. 2-Adjustments to book record to annualize and normalize under present rates. 3-Income statement under present rates after adjustment in Col. 2 4-Adjustment to Col. 3 for revenue increase requested. 5-Income statement under requested rates. a. Expenses may be summarized by the following expense classifications for purposes of this statement: Operating Expenses (by category) Depreciation Amortization Taxes, Other than Income Taxes Total Operating Expense Operating Income Before Taxes Federal Taxes State Taxes Deferred Federal Deferred State Income Tax Credits Other Credits Other Credits and Charges, etc. Total Income Taxes Net Utility Operating Income Other Income & Deductions Other Income Detailed listing of Other Income used in Tax Calculation Other Income Deduction Detailed Listing Taxes Applicable to Other Income and Deductions	2 2	3 4	102	3	Komenda Komenda

Columbia Gas of Pennsylvania, Inc.
Docket No. R-2024-3046519
Referenced by Commission Regulations

Commission Regulation Number	Commission Regulation	Historic Test Year Twelve Months Ended <u>November 30, 2023</u>		Fully Projected Future Test Year Twelve Months Ended <u>December 31, 2025</u>		Witness
		<u>Exhibit</u>	<u>Schedule</u>	<u>Exhibit</u>	<u>Schedule</u>	
	Listing Income Before Interest Charges Listing of all types of Interest Charges and all amortization of Premiums and/or Discounts and expenses on Debt issues Total Interest Net Income After Interest Charges (Footnote each adjustment to the above statements with explanation in sufficient clarifying detail.)	2	3, 4			Komenda
53.53.III.A18	Provide comparative operating statements for the test year and the immediately preceding 12 months showing increases and decreases between the two periods. These statements should supply detailed explanation of the causes of the major variances between the test year and preceding year by detailed account number.	2	5	102	4	Komenda
53.53.III.A19	List extraordinary property losses as a separate item, not included in operating expenses or depreciation and amortization. Sufficient supporting data must be provided.	13	5	113	3	Komenda
53.53.III.A20	Supply detailed calculations of amortization of rate case expense, including supporting data for outside services rendered. Provide the items comprising the rate case expense claim (include the actual billings or invoices in support of each kind of rate case expense), the items comprising the actual expenses of prior rate cases and the unamortized balances.	4	4	104	4	Komenda
53.53.III.A21	Submit detailed computation of adjustments to operating expenses for salary, wage and fringe benefit increases (union and non-union merit, progression, promotion and general) granted during the test year and six months subsequent to the test year. Supply data showing for the test year: a. Actual payroll expense (regular and overtime separately) by categories of operating expenses. i.e. maintenance, operating transmission, distribution, other. b. Date, percentage increase, and annual amount of each general payroll increase during the test year. c. Dates and annual amounts of merit increases or management salary adjustments. d. Total annual payroll increases in the test year e. Proof that the actual payroll plus the increases equal the payroll expense claimed in the supporting data (by categories of expenses). f. Detailed list of employee benefits and cost thereof for union and non-union personnel. Any specific benefits for electives and officers should also be included, and cost thereof. g. Support the annualized pension cost figures (i) State whether these figures include any unfunded pension costs. Explain. (ii) Provide latest actuarial study used for determining pension accrual rates. h. Submit a schedule showing any deferred income and consultant fee to corporate officers or employees.	4	5	104	5	Komenda
53.53.III.A22	Supply an exhibit showing an analysis, by functional accounts, of the charges by affiliates (Service Corporations, etc.) for services rendered included in the operating expenses of the filing company for the 12-month period ended prior to the test year. a. Supply a copy of contracts, if applicable. b. Explain the nature of the services provided. c. Explain basis on which charges are made. d. If charges allocated, identify allocation factors used.	4	11	104	9	Komenda

Columbia Gas of Pennsylvania, Inc.
Docket No. R-2024-3046519
Referenced by Commission Regulations

Commission Regulation Number	Commission Regulation	Historic Test Year Twelve Months Ended <u>November 30, 2023</u>		Fully Projected Future Test Year Twelve Months Ended <u>December 31, 2025</u>		Witness
		<u>Exhibit</u>	<u>Schedule</u>	<u>Exhibit</u>	<u>Schedule</u>	
53.53.III.A23	e. Supply the components and amounts comprising the expense in this account. f. Provide details of initial source of charge and reason thereof. Describe costs relative to leasing equipment, computer rentals, and office space, including terms and conditions of the lease. State method for calculating monthly or annual payments.	4	12	104	9	Komenda
53.53.III.A24	Submit detailed calculations (or best estimates) of the cost resulting from major storm damage.	4	13	104	9	Komenda
53.53.III.A25	Submit details of expenditures for advertising (National and Institutional and Local media). Provide a schedule of advertising expense by major media categories for the test year and the prior two comparable years with respect to: a. Public health and safety b. Conservation of energy c. Explanation of Billing Practices. Rates, etc. d. Provision of factual and objective data programs in educational institutions e. Other advertising programs f. Total advertising expense	4	8	104	6	Komenda
53.53.III.A26	Provide a list of reports, data, or statements requested by and submitted to the Commission during and subsequent to the test year.	14	1	114	1	Danhires
53.53.III.A27	Prepare a detailed schedule for the test year showing types of social and service organization memberships paid for by the Company and the cost thereof.	4	14	104	9	Komenda
53.53.III.A28	Submit a schedule showing, by major components, the expenditures associated with Outside Services Employed, Regulatory Commission Expenses and Miscellaneous General Expenses, for the test year and prior two comparable years.	4	14	104	9	Komenda
53.53.III.A29	Submit details of information covering research and development expenditures, including major projects within the company and forecasted company programs.	4	9	104	7	Komenda
53.53.III.A30	Provide a detailed schedule of all charitable and civic contributions by recipient and amount for the test year.	4	15	104	9	Komenda
53.53.III.A31	Provide a detailed analysis of Special Services-Account 795.	4	14	104	9	Komenda
53.53.III.A32	Provide a detailed analysis of Miscellaneous General Expense-Account No. 801.	4	14	104	9	Komenda
53.53.III.A33	Provide a labor productivity schedule.	4	10	104	8	Komenda
53.53.III.A34	List and explain all non-recurring abnormal or extraordinary expenses incurred in the test year which will not be present in future years.	4	16	104	9	Komenda
53.53.III.A35	List and explain all expenses included in the test year which do not occur yearly but are of a nature that they do occur over an extended period of years. (e.g.,-Non-yearly maintenance programs, etc.) [Responses shall be submitted and identified as exhibits.]	4	16	104	9	Komenda
53.53.III.A36	Using the adjusted year's expenses under present rates as a base, give detail necessary for clarification of all expense adjustments. Give clarifying detail for such adjustments that occur due to changes in accounting procedure, such as charging a particular expense to a different account than was used previously. Explain any extraordinary declines in expense due to such change of account use.	4	16	104	9	Komenda

Columbia Gas of Pennsylvania, Inc.
Docket No. R-2024-3046519
Referenced by Commission Regulations

Commission Regulation Number	Commission Regulation	Historic Test Year Twelve Months Ended <u>November 30, 2023</u>		Fully Projected Future Test Year Twelve Months Ended <u>December 31, 2025</u>		Witness
		<u>Exhibit</u>	<u>Schedule</u>	<u>Exhibit</u>	<u>Schedule</u>	
53.53.III.A37	Indicate the expenses that are recorded in the test year, which are due to the placement in operating service of major plant additions or the removal of major plant from operating service, and estimate the expense that will be incurred on a full-year's operation.	4	16	104	9	Komenda
53.53.III.A38	Submit a statement of past and anticipated changes, since the previous rate case, in major accounting procedures.	4	16	104	9	Komenda
53.53.III.A39	Identify the specific witness for all statements and schedules of revenues, expenses, taxes, property, valuation, etc.	13	3	113	3	Kempic
53.53.III.A40	Adjustments which are estimated shall be fully supported by basic information reasonably necessary.	13	4	113	3	Komenda
53.53.III.A41	Submit a statement explaining the derivation of the amounts used for projecting future test year level of operations and submit appropriate schedules supporting the projected test year level of operations.	13	4	113	3	Komenda
53.53.III.A42	If a company has separate operating divisions, an income statement must be shown for each division, plus an income statement for company as a whole.	2	6	102	5	Komenda
53.53.III.A43	If a company's business extends into different states or jurisdictions, then statements must be shown listing Pennsylvania jurisdictional data, other state data and federal data separately and jointly (Balance sheets and operating accounts)	2	6	102	5	Komenda
53.53.III.A44	Ratios, percentages, allocations and averages used in adjustments must be fully supported and identified as to source.	13	4	113	3	Komenda
53.53.III.A45	Provide an explanation of any differences between the basis or procedure used in allocations of revenues, expenses, depreciation and taxes in the current rate case and that used in the prior rate case.	13	4	113	3	Komenda
53.53.III.A46	Supply a copy of internal and independent audit reports of the test year and prior calendar year, noting any exceptions and recommendations and disposition thereof.	13	4	113	3	Komenda
53.53.III.A47	Submit a schedule showing rate of return on facilities allocated to serve wholesale customers.	11		111		Johnson
53.53.III.A48	Provide a copy of the latest capital stock tax report and the latest capital stock tax settlement.	6	3	106	3	Harding
53.53.III.A49	Submit details of calculations for Taxes, Other than Income where a company is assessed taxes for doing business in another state, or on its property located in another state.	6	4	106	3	Harding
53.53.III.A50	Provide a schedule of federal and Pennsylvania taxes, other than income taxes, calculated on the basis of test year per books, pro forma at present rates, and pro forma at proposed rates, to include the following categories: a. social security b. unemployment c. capital stock d. public utility realty e. PUC assessment f. other property g. any other appropriate categories	6	2	106	2	Harding
53.53.III.A51	Submit a schedule showing for the last five years the income tax refunds, plus interest (net of taxes), received from the federal government due to prior years' claims.	7		107		Harding

Columbia Gas of Pennsylvania, Inc.
Docket No. R-2024-3046519
Referenced by Commission Regulations

Commission Regulation Number	Commission Regulation	Historic Test Year Twelve Months Ended <u>November 30, 2023</u>		Fully Projected Future Test Year Twelve Months Ended <u>December 31, 2025</u>		Witness
		<u>Exhibit</u>	<u>Schedule</u>	<u>Exhibit</u>	<u>Schedule</u>	
53.53.III.A52	Provide detailed computations showing the deferred income taxes derived by using accelerated tax depreciation applicable to post-1969 utility property increases productive capacity, and ADR rates on property. (Separate between state and federal, also rate used).	7		107		Harding
	a. State whether tax depreciation is based on all rate base items claimed as of the end of the test year, and whether it is the annual tax depreciation at the end of the test year. b. Reconcile any difference between the deferred tax balance, as shown as a reduction to measures of value (rate base), and the deferred tax balance as shown on the balance sheet.	7		107		Harding
53.53.III.A53	Submit a schedule showing a breakdown of the deferred income taxes by state and federal per books, pro-forma existing rates, and under proposed rates.	7		107		Harding
53.53.III.A54	Submit a schedule showing a breakdown of accumulated investment tax (credits 3 percent, 4 percent, 7 percent, 10 percent and 11 percent), together with details of methods used to write-off the unamortized balances.	7		107		Harding
53.53.III.A55	Submit a schedule showing the adjustments for taxable net income per books (including below-the-line items) and pro-forma under existing rates, together with an explanation of any difference between the adjustments. Indicate charitable donations and contributions in the tax calculation for rate making purposes.	7		107		Harding
53.53.III.A56	Submit detailed calculations supporting taxable income before state and federal income taxes where the income tax is subject to allocation due to operations in another state, or due to operation of other taxable utility or non-utility business, or by operating divisions or areas.	7		107		Harding
53.53.III.A57	Submit detailed calculations showing the derivation of deferred income taxes for amortization of repair allowance if such policy is followed. [Note: Submit additional schedules if the company has more than one accounting area.]	7		107		Harding
53.53.III.A58	Furnish a breakdown of major items comprising prepaid and deferred income tax charges and other deferred income tax credits and reserves by accounting areas.	7		107		Harding
53.53.III.A59	Provide details of the Federal Surtax Credit allocated to the Pennsylvania jurisdictional area, if applicable.	7		107		Harding
53.53.III.A60	Explain the reason for the use of cost of removal of any retired plant figures in the income tax calculations.	7		107		Harding
53.53.III.A61	Submit the corresponding data applicable to Pennsylvania Corporate Income Tax deferment. a. Show the amounts of straight line tax depreciation and accelerated tax depreciation, the difference between which gave rise to the normalizing tax charged back to the test year operating statement. b. Show normalization for both Federal and State Income Taxes. c. Show tax rates used to calculate tax deferment amount.	7		107		Harding

Columbia Gas of Pennsylvania, Inc.
Docket No. R-2024-3046519
Referenced by Commission Regulations

Commission Regulation Number	Commission Regulation	Historic Test Year Twelve Months Ended <u>November 30, 2023</u>		Fully Projected Future Test Year Twelve Months Ended <u>December 31, 2025</u>		Witness
		<u>Exhibit</u>	<u>Schedule</u>	<u>Exhibit</u>	<u>Schedule</u>	
53.53.III.A62	Provide the accelerated tax depreciation and the book depreciation used to calculate test year deferrals in amounts segregated as follows: For: a. Property installed prior to 1970. b. Property installed subsequent to 1969 (indicate increasing capacity additions and no increasing capacity additions).	7		107		Harding
53.53.III.A63	State whether all tax savings due to accelerated depreciation on property installed prior to 1970 have been passed through to income. (If not, explain).	7		107		Harding
53.53.III.A64	Show any income tax loss/gain carryovers from previous years that may effect test year income taxes or future year income taxes. Show loss/gain carryovers by years of origin and amounts remaining by years at the end of the test year.	7		107		Harding
53.53.III.A65	State whether the company eliminates any tax savings by the payment of actual interest on construction work in progress not in rate base claim. If response is affirmative: a. Set forth amount of construction claimed in this tax savings reduction. Explain the basis for this amount. b. Explain the manner in which the debt portion of this construction is determined for purposes of the deferral calculations. c. State the interest rate used to calculate interest on this construction debt portion, and the manner in which it is derived. d. Provide details of calculation to determine tax saving reduction. State whether state taxes are increased to reflect the construction interest elimination.	7		107		Harding
53.53.III.A66	Provide a detailed analysis of Taxes Accrued per books as of the test year date. Also supply the basis for the accrual and the amount of taxes accrued monthly.	7		107		Harding
53.53.III.A67	For the test year as recorded on test year operating statement: a. Supply the amount of federal income taxes actually paid. b. Supply the amount of the federal income tax normalizing charge to tax expense due to excess of accelerated tax depreciation over book depreciation. c. Supply the normalizing tax charge to federal income taxes for the 10% Job Development Credit during test year. d. Provide the amount of the credit of federal income taxes due to the amortization or normalizing yearly debit to the reserve for the 10% Job Development Credit. e. Provide the amount of the credit to federal income taxes for the normalizing of any 3% Investment Tax Credit Reserve that may remain on the utility books.	7		107		Harding
53.53.III.A68	Provide the debit and credit in the test year to the Deferred Taxes due to Accelerated Depreciation for federal income tax, and provide the debit and credit for the Job Development Credits (whatever account) for test year.	7		107		Harding

Columbia Gas of Pennsylvania, Inc.
Docket No. R-2024-3046519
Referenced by Commission Regulations

Commission Regulation Number	Commission Regulation	Historic Test Year Twelve Months Ended <u>November 30, 2023</u>		Fully Projected Future Test Year Twelve Months Ended <u>December 31, 2025</u>		Witness
		<u>Exhibit</u>	<u>Schedule</u>	<u>Exhibit</u>	<u>Schedule</u>	
53.53.III.A69	Reconcile all data given in answers to questions on income taxes charged on the test year operating statement with regard to income taxes paid, income taxes charged because of normalization and credits due to yearly write-offs of past years' income tax deferrals, and from normalization of investment tax and development credits. (Both state and federal income taxes.)	7		107		Harding
53.53.III.A70	With respect to determination of income taxes, federal and state: a. Show income tax results of the annualizing and normalizing adjustments to the test year record before any rate increase. b. Show income taxes for the annualized and normalized test year. c. Show income tax effect of the rate increase requested. d. Show income taxes for the normalized and annualized test year after application of the full rate increase. [It is imperative that continuity exists between the income tax calculations as recorded for the test year and the final income tax calculation under proposed rates. If the company has more than one accounting area, then additional separate worksheets must be provided in addition to those for total company.]	7		107		Harding
53.53.III.A71	In adjusting the test year to an annualized year under present rates, explain any changes that may be due to book or tax depreciation change and to debits and credits to income tax expense due to accelerated depreciation, deferred taxes, job development credits, tax refunds or other items. (The above refers only the adjustments going from recorded test year to annualized test year).	7		107		Harding
<u>53.53.III.E</u>	<u>53.53.III.BALANCE SHEET AND OPERATING STATEMENT</u> <u>E. GAS UTILITIES</u>					
53.53.III.E.1	If Unrecovered Fuel Cost policy is implemented, provide the following: a. State manner in which amount of Unrecovered Fuel Cost on balance sheet at the end of the test year was determined, and the month in test year in which such fuel expense was actually incurred. Provide amount of adjustment made on the rate case operating account for test year-end unrecovered fuel cost. (If different than balance sheet amount, explain.) b. Provide amount of Unrecovered Fuel Cost that appeared on the balance sheet at the opening date of the test year, and the manner in which it was determined. State whether this amount is in the test year operating account..	1	18	101		Komenda
53.53.III.E.2	Provide details of items and amounts comprising the accounting entries for Deferred Fuel Cost at the beginning and end of the test year.	1	18	101		Komenda
53.53.III.E.3	Submit a schedule showing a reconciliation of test year MCF sales and line losses. List all amounts of gas purchased, manufactured and transported.	10	7	110	7	Battig
53.53.III.E.4	Provide detailed calculations substantiating the adjustment to revenues for annualization of changes in number of customers and annualization of changes in volume sold for all customers for the test year. a. Break down changes in number of customers by rate schedules. b. If an annualization adjustment for changes in customers and changes in volume sold is not submitted, please explain.	3		103		Battig
53.53.III.E.5	Submit a schedule showing the sources of gas supply associated with annualized MCF sales.	12	1	112	1	Battig

Columbia Gas of Pennsylvania, Inc.
Docket No. R-2024-3046519
Referenced by Commission Regulations

Commission Regulation Number	Commission Regulation	Historic Test Year Twelve Months Ended <u>November 30, 2023</u>		Fully Projected Future Test Year Twelve Months Ended <u>December 31, 2025</u>		Witness
		<u>Exhibit</u>	<u>Schedule</u>	<u>Exhibit</u>	<u>Schedule</u>	
53.53.III.E.6	Supply, by classification. Operating Revenues - Miscellaneous for test year	3		103		Battig
53.53.III.E.7	Provide details of respondent's attempts to recover uncollectible and delinquent accounts.	16		116	1	Battig
53.53.III.E.8	Describe how the net billing and gross billing is determined. For example, if the net billing is based on the rate blocks plus FCA and STA, and the gross billing is determined by a percentage increase (1, 3, 5 percent), then state whether the percentage increase is being applied to all three items of revenue - rate blocks plus FCA and STA.	3		103		Battig
53.53.III.E.9	Describe the procedures involved in determining whether forfeited discounts or penalties are applied to customers billing.	3		103		Battig
53.53.III.E.10	Provide annualization of revenues as a result of rate changes occurring during the test year, at the level of operations as of end of the test year.	3		103		Battig
53.53.III.E.11	Provide a detailed billing analysis supporting present and proposed rates by customer classification and/or tariff rate schedule.	3		103		Battig
53.53.III.E.12	Provide a schedule showing residential and commercial heating sales by unit (MCF) per month and degree days for the test year and three preceding twelve month periods.	10	1	110	1	Girata
53.53.III.E.13	Provide a schedule of present and proposed tariff rates showing dollar change and percent of change by block. Also, provide an explanation of any change in block structure and the reasons therefore.	3		103		Battig
53.53.III.E.14	Provide the following statements and schedules. The schedules and statements for the test year portion should be reconciled with the summary operating statement. a. An operating revenues summary for the test year and the year preceding the test year showing the following (Gas MCF): (i) For each major classification of customers (a) MCF sales (b) Dollar Revenues (c) Forfeited Discounts (Total if not available by classification) (d) Other and Miscellaneous revenues that are to be taken into the utility operating account along with their related costs and expenses. (ii) A detailed explanation of all annualizing and normalizing adjustments showing method utilized and amounts and rates used in calculation to arrive at adjustment. (iii) Segregate, from recorded revenues from the test year, the amount of revenues that are contained therein, by appropriate revenue categories, from: (a) Fuel Adjustment Surcharge (b) State Tax Surcharge (c) Any other surcharge being used to collect revenues. (d) Provide explanations if any of the surcharges are not applicable to respondent's operations. [The schedule should also show number of customers and unit of sales (Mcf), and should provide number of customers by service classification at beginning and end of test year.]	3		103		Battig

Columbia Gas of Pennsylvania, Inc.
Docket No. R-2024-3046519
Referenced by Commission Regulations

Commission Regulation Number	Commission Regulation	Historic Test Year Twelve Months Ended <u>November 30, 2023</u>		Fully Projected Future Test Year Twelve Months Ended <u>December 31, 2025</u>		Witness
		<u>Exhibit</u>	<u>Schedule</u>	<u>Exhibit</u>	<u>Schedule</u>	
	b. Provide details of sales for resale, based on periods five years before and projections for five years after the test year, and for the test year. List customers, Mcf sold, revenues received, source of Mcf sold (storage gas, pipeline gas, manufactured gas, natural or synthetic), contracted or spot sales, whether sales are to affiliated companies, and any other pertinent information.	3		103		Battig
53.53.III.E.15	State manner in which revenues are being presented for ratemaking purposes: a. Accrued Revenues b. Billed Revenues c. Cash Revenues Provide details of the method followed.	3		103		Battig
53.53.III.E.16	If revenue accruing entries are made on the books at end of each fiscal period, give entries made accordingly at the end of the test year and at the beginning of the year. State whether they are reversed for ratemaking purposes.	2	7	102	6	Komenda
53.53.III.E.17	State whether any adjustments have been made to expenses in order to present such expenses on a basis comparable to the manner in which revenues are presented in this proceeding (i.e.- accrued, billed or cash).	4	1	104	1	Komenda
53.53.III.E.18	If the utility has a Fuel Adjustment Clause: a. State the base fuel cost per MCF chargeable against basic customers' rates during the test year. If there was any change in this basic fuel charge during the test year, give details and explanation thereof. b. State the amount in which the fuel adjustment clause cost per MCF exceeds the fuel cost per MCF charged in base rates at the end of the test year. c. If fuel cost deferment is used at the end of the test year, give (i) The amount of deferred fuel cost contained in the operating statement that was deferred from the 12-month operating period immediately preceding the test year. (ii) The amount of deferred fuel cost that was removed from the test period and deferred to the period immediately following the test year. d. State the amount of Fuel Adjustment Clause revenues credited to the test year operating account. e. State the amount of fuel cost charged to the operating expense account in the test year which is the basis of Fuel Adjustment Clause billings to customers in that year. Provide summary details of this charge f. From the recorded test year operating account, remove the Fuel Adjustment Clause Revenues. Also remove from the test year recorded operating account the excess of fuel cost over base rate fuel charges, which is the basis for the Fuel Adjustment charges. Explain any differences between FAC Revenues and excess fuel costs. [The above is intended to limit the operating account to existing customers' base rate revenues and expense deductions relative thereto].	12	2	112	2	Battig
53.53.III.E.19	Provide growth patterns of usage and customer numbers per rate class, using historical and projected data.	10	2	110	2	Girata
53.53.III.E.20	Provide, for test year only, a schedule by tariff rates and by service classifications showing proposed increase and percent of increase.	3		103		Battig

Columbia Gas of Pennsylvania, Inc.
Docket No. R-2024-3046519
Referenced by Commission Regulations

Commission Regulation Number	Commission Regulation	Historic Test Year Twelve Months Ended <u>November 30, 2023</u>		Fully Projected Future Test Year Twelve Months Ended <u>December 31, 2025</u>		Witness
		<u>Exhibit</u>	<u>Schedule</u>	<u>Exhibit</u>	<u>Schedule</u>	
53.53.III.E.21	If a gas company is affiliated with another utility segment, such as a water or electric segment, explain the effects, if any, upon allocation factors used in the gas rate filing of current or recent rate increases allowed to the other utility segment (or segments) of the company.	2	8	102	7	Komenda
53.53.III.E.22	Provide supporting data detailing curtailment adjustments, procedures and policies.	10	3	110	3	Battig
53.53.III.E.23	Submit a schedule showing fuel cost in excess of base compared to fuel cost recovery for the period two months prior to test year and the test year	12	3	112	2	Battig
53.53.III.E.24	Supply a detailed analysis of Purchased Gas for the test year and the twelve month period prior to the test year.	12	4	112	2	Battig
53.53.III.E.25	Submit calculations supporting energy cost per MCF and operating ratio used to determine increase in costs other than production to serve additional load.	12	4	112	2	Battig
53.53.III.E.26	Submit detailed calculations for bulk gas transmission service costs under supply and/or interconnection agreements.	12	4	112	2	Battig
53.53.III.E.27	Submit a schedule for gas producing units retired or scheduled for retirement subsequent to the test year showing station, units, MCF capacity, hours of operation during test year, net output produced and cents/MCF of maintenance and fuel expenses.	13	6	113	4	Covert
53.53.III.E.28	Provide a statement explaining the details of firm gas purchase (long-term) contracts with affiliated and nonaffiliated utilities, including determination of costs, terms of contract, and other pertinent information.	17		117		Battig
53.53.III.E.29	Provide intrastate operations percentages by expense categories for two years prior to the test year.	4	17	104	9	Komenda
53.53.III.E.30	Provide a schedule showing suppliers, MCF purchased, cost (small purchases from independent suppliers may be grouped); emergency purchases, listing same information; curtailments during the year; gas put into and taken out of storage; line loss, and any other gas input or output not in the ordinary course of business.	12	4	112	2	Battig
53.53.III.E.31	Provide a schedule showing the determination of the fuel costs included in the base cost of fuel.	12	5	112	2	Battig
53.53.III.E.32	Provide a schedule showing the calculation of any deferred fuel costs shown in Account 174. Also, explain the accounting, with supporting detail, for any associated income taxes.	1	19	101		Komenda
53.53.III.E.33	Submit a schedule showing maintenance expenses, gross plant and the relation of maintenance expenses thereto as follows. (i) Gas Production Maintenance Expenses per MCF production, per \$1,000 MCF production, and per \$1,000 of Gross Production Plant; (ii) Transmission Maintenance Expenses per MMCF mile and per \$1,000 of Gross Transmission Plant; (iii) Distribution Maintenance Expenses per customer and per \$1,000 of Gross Distribution Plant; (iv) Storage Maintenance Expenses per MMCF of Storage Capacity and per \$1,000 of Gross Storage Plant. This schedule shall include three years prior to the test year, the test year and one year's projection beyond the test year.	4	18	104	9	Komenda
53.53.III.E.34	Prepare a 3-column schedule of expenses, as described below for the following periods (supply sub-accounts, if significant, to clarify basic accounts): a. Column 1 - Test Year b. Column 2 and 3 - The two previous years	4	3 19	104	3	Komenda

Columbia Gas of Pennsylvania, Inc.
Docket No. R-2024-3046519
Referenced by Commission Regulations

Commission Regulation Number	Commission Regulation	Historic Test Year Twelve Months Ended <u>November 30, 2023</u>		Fully Projected Future Test Year Twelve Months Ended <u>December 31, 2025</u>		Witness
		<u>Exhibit</u>	<u>Schedule</u>	<u>Exhibit</u>	<u>Schedule</u>	
	Provide the annual recorded expense by accounts. (Identify all accounts used but not specifically listed below.)					
53.53.III.E.35	Submit a schedule showing the Gross Receipts Tax Base used in computing Pennsylvania Gross Receipts Tax Adjustment.	6	1	106	1	Harding
53.53.III.E.36	State the amount of gas, in MCF, obtained through various suppliers in past years.	12	4	112	2	Battig
53.53.III.E.37	In determining pro forma expense, exclude cost of gas adjustments applicable to fuel adjustment clause and exclude fuel adjustment clause revenues, so that the operating statement is on the basis of base rates only.	3		103		Battig
53.53.III.E.38	Identify company's policy with respect to replacing customers lost through attrition.	10	4	110	4	Battig
53.53.III.E.39	Identify procedures developed to govern relationship between the respondent and potential customers - i.e., basically expansion, alternate energy requirements, availability of supply, availability of distribution facilities, ownership of metering and related facilities.	10	4	110	4	Danhires
<u>53.53.IV.B</u>	<u>53.53.IV. RATE STRUCTURE</u> <u>B. GAS UTILITIES</u> Each gas utility shall submit the following simultaneously with any rate increase filing:					
53.53.IV.B.1	Provide a Cost of Service Study showing the rate of return under the present and proposed tariffs for all customer classifications. The study should include a summary of the allocated measures of value, operating revenues, operating expenses and net return for each of the customer classifications at original cost and at the 5-year trended original cost.	11		111	1 - 3	Johnson
53.53.IV.B.2	Provide a statement of testimony describing the complete methodology of the cost of service study.	11		111		Johnson
53.53.IV.B.3	Provide a complete description and back-up calculations for all allocation factors.	11		111	4	Johnson
53.53.IV.B.4	Provide an exhibit for each customer classification showing the following data for the test year and the four previous years: a. The maximum coincident peak day demand. b. The maximum coincident 3-day peak day demand. c. The average monthly consumption in Mcf during the Primary Heating Season (November-March). d. The average monthly consumption in Mcf during the Non-heating season (April-October). e. The average daily consumption in Mcf for each 12-month period	10	5	110	5	Girata
53.53.IV.B.5	Submit a Bill Frequency Analysis for each rate. The analysis should include the rate schedule and block interval, the number of bills at each interval, the cumulative number of bills at each interval, the Mcf or therms at each interval, the cumulative Mcf or therms at each interval, the accumulation of Mcf or therms passing through each interval, and the revenue at each interval for both the present rate and the proposed rates. The analysis should show only those revenues collected from the basic tariff.	11		111		Battig
53.53.IV.B.6	Supply copies of all present and proposed Gas Tariffs.	14	2	114	1	Danhires
53.53.IV.B.7	Supply a graph of present and proposed base rates on hyperbolic cross section paper.	11		111	5	Battig

Columbia Gas of Pennsylvania, Inc.
Docket No. R-2024-3046519
Referenced by Commission Regulations

Commission Regulation Number	Commission Regulation	Historic Test Year Twelve Months Ended <u>November 30, 2023</u>		Fully Projected Future Test Year Twelve Months Ended <u>December 31, 2025</u>		Witness
		<u>Exhibit</u>	<u>Schedule</u>	<u>Exhibit</u>	<u>Schedule</u>	
53.53.IV.B.8	Supply a map showing the Gas System Facilities and Gas Service Areas. The map should include transmission lines, distribution lines, other companies' lines interconnecting with the interconnecting points clearly designated, major compressor stations, gas storage and gas storage lines. The normal direction of gas flow within the transmission system should be indicated by arrows. Separate service areas within the system should be clearly designated.	15	2	115		Danhires
53.53.IV.B.9	Supply a cost analysis supporting minimum charges for all rate schedules.	11		111	2 - 3	Johnson
53.53.IV.B.10	Supply a cost analysis supporting demand charges for all tariffs which contain demand charges.	11		111		Johnson
53.53.IV.B.11	Supply the net fuel clause adjustment by month for the test year.	12	6	112	2	Battig
53.53.IV.B.12	Supply a tabulation of base rate bills for each rate schedule comparing the existing rates to proposed rates. The tabulation should show the dollar difference and the per cent increase or decrease.	11		111	6	Battig
53.53.IV.B.13	Submit the projected demands for all customer classes for both purchased and produced gas for the three years following the test year filing.	10	6	110	6	Girata
53.53.IV.B.14	Supply an exhibit showing the gas deliveries to each customer class for the most recent 24 month period. The exhibit should identify the source of the gas, such as "purchased" (pipeline), "production" (include purchases from local producers), "storage withdrawal", "propane/air", and "unaccounted for".	10	7	110	7	Battig
<u>53.62</u>	<u>53.62 RECOVERY OF FUEL COSTS BY GAS UTILITIES</u> In addition to information otherwise required to be filed by a jurisdictional natural gas distributor with gross intrastate annual operating revenues in excess of \$40 million seeking a change in its base rates, each gas utility must also file updates to the information required by &53.64(c) (relating to filing requirements for natural gas distributors with gross intrastate annual operating revenues in excess of \$40 million). In the case of a utility purchasing gas as defined at &53..61 (a) (relating to purpose) from an affiliated interest, it shall also file updates to the information required at &53.65 (relating to special provisions relating to natural gas distributors with gross interstate annual operating revenues in excess of \$40 million with affiliated interests). These updates shall be made at the time the base rate case under 66 Pa.C.S. 1308 (relating to voluntary changes in rates) is originally filed. Deficiencies in filing will be treated as set forth at &53.51 (c) (relating to general).					
	Weather Normalization Adjustment	10	8	110	8	Girata
	Volumetric Portion of Load Growth Adjustment	10	9	110	9	Girata
	Estimated Number of Bills and Normalized Sales Volumes	10	9	110	9	Girata
	Future Test Year Sales Forecast	10	9	110	10	Girata
	Adjustment to Purchase Gas Expense	12	7	112	3	Battig
	Recovery of Fuel Costs by Gas Utilities (1307-F)	12	8	112	4	Battig

COLUMBIA GAS OF PENNSYLVANIA, INC
53.53 III. BALANCE SHEET AND OPERATING STATEMENT
A. ALL UTILITIES

40. Adjustments which are estimated shall be fully supported by basic information reasonably necessary.

Response: All adjustments made were based on annualizing and normalizing the 12 months ended November 30, 2023. The derivation and support behind the adjustments are shown on the following exhibits:

Exhibit No. 2	Income Statement
Exhibit No. 3	Revenues
Exhibit No. 4	Expenses
Exhibit No. 5	Depreciation
Exhibit No. 6	Taxes Other Than Income Taxes
Exhibit No. 7	Income Taxes
Exhibit No. 8	Measures of Value

41. Submit a statement explaining the derivation of the amounts used for projecting future test year level of operations and submit appropriate schedules supporting the projected test year level of operations.

Response: Exhibits explaining the derivation of the amounts used for projecting a future test year (12 months ending November 30, 2024) and a fully projected future test year (12 months ended December 31, 2025) are:

Exhibit No. 102	Income Statement
Exhibit No. 103	Revenues
Exhibit No. 104	Expenses
Exhibit No. 105	Depreciation
Exhibit No. 106	Taxes Other Than Income Taxes
Exhibit No. 107	Income Taxes
Exhibit No. 108	Measures of Value

COLUMBIA GAS OF PENNSYLVANIA, INC
53.53 III. BALANCE SHEET AND OPERATING STATEMENT
A. ALL UTILITIES

44. Ratios, percentages, allocations and averages used in adjustments must be fully supported and identified as to source.

Response: When allocation factors are used, they are identified on the appropriate exhibit.

45. Provide an explanation of any differences between the basis or procedure used in allocations of revenues, expenses, depreciation and taxes in the current rate case and that used in the prior rate case.

Response: There are no differences.

46. Supply a copy of internal and independent audit reports of the test year and prior calendar year, noting any exceptions and recommendations and disposition thereof.

Response: Please see Exhibit 13, Schedule 4 Attachment A for copies of internal audits. There were no independent audit reports performed specifically for Columbia Gas of Pennsylvania during the test year and prior calendar year.

	Date of Report	Audit	Report
1	1/13/2022	Bangs Fabrication Shop	Yes
2	1/18/2022	Security Baselines	Yes
3	2/17/2022	Environmental Function General Controls	Yes
4	3/1/2022	Identify and Access Management Execution	Yes
5	3/2/2022	Integration Center General Controls	Yes
6	3/2/2022	NiSource Next Digital Field Enablement	Yes
7	3/10/2022	Operations General Controls	Yes
8	4/18/2022	Critical Process Disaster Recovery and Business Continuity	Yes
9	4/29/2022	Sensitive Customer Data Protection	Yes
10	5/23/2022	Capital Accounting	Yes
11	5/23/2022	Distributive Information System Customer Billing General Controls	Yes
12	6/10/2022	Operator Qualification Management	Yes
13	7/13/2022	Management of Change Advisory Review	Yes
14	9/30/2022	Environmental Data Quality and Reporting Controls	Yes
15	10/7/2022	Manual Billing Processes	Yes
16	10/13/2022	Gas Standards Management Advisory Review	Yes
17	1/6/2023	PHMSA Megal Rule Compliance Activities	Yes
18	1/17/2023	Treasury Operations General Controls	Yes
19	1/17/2023	Gas Supply General Controls	Yes
20	1/18/2023	Customer Credit and Collections Processes	Yes
21	3/8/2023	GIS IT General Controls	Yes
22	3/8/2023	Source to Pay General Controls	Yes
23	3/9/2023	Cybersecurity Cloud Computing Controls	Yes
24	3/10/2023	Corrective Action Program Processes	Yes
25	5/4/2023	Gas Engineering Materials Quality Processes	Yes
26	5/5/2023	Data Center Operations	Yes
27	5/16/2023	Customer Connect Processes	Yes
28	5/17/2023	Technology Capital Accounting	Yes
29	5/17/2023	Technology Project Management Office Processes	Yes
30	7/31/2023	Customer Contact Center Technology Controls	Yes
31	7/31/2023	Key Vendor Governance	Yes
32	9/13/2023	Remote Access & Firewall Security Controls	Yes
33	10/16/2023	Payroll General Controls	Yes
34	10/16/2023	Inventory Management General Controls	Yes
A	8/2/2022	Cybersecurity TSA Directives (Attorney-Client Privilege)	No

NiSource Inc.
Bangs Fabrication Shop
Internal Audit Report

Distribution

Beneficiaries

Daniel Creekmur

William Mojica

James Zucal

Other Key Personnel

David Dunn

Ron Parsons

For Information

Shawn Anderson

Donald Brown

Kimberly Cuccia

Joseph Hamrock

Charles Shafer

Violet Sistovaris

Pablo Vegas

January 13, 2021

Internal Audit Report

Background

The NiSource Inc. (NiSource or the Company) Bangs, Ohio Fabrication Shop (BANGS) supports Northern Indiana Public Service Company LLC (NIPSCO) and Columbia Distribution Companies (CDC) gas operations by custom-fabricating components used to support gas installation and maintenance activities. In a typical year, BANGS completes approximately one thousand orders. Upon receiving an order for a fabricated component, BANGS personnel test the material that will be utilized for the order to ensure it meets established quality standards. After components are fabricated, and prior to completing the order, components are tested again to ensure tolerance guidelines established by the requesting engineer, as well as the associated gas standards, are met.

In April 2020, BANGS obtained International Standards Order (ISO) 9001 certification, which is awarded based on the Company's ability to consistently provide products and services that meet customer and regulatory requirements and demonstrate continuous improvement. To maintain ISO 9001 certification, BANGS is subject to periodic surveillance audits and a full recertification review every three years.

Audit Objective, Approach, and Coverage

The objective of this management-requested, risk-based internal audit was to provide an independent evaluation of the adequacy, effectiveness and efficiency of controls used to enable and manage key BANGS activities. We conducted detailed process assessments and sample-based transactional testing in the highest-risk areas. The audit review period was January 2021 through December 2021.

During the audit, we specifically evaluated:

- The design of processes, procedures and controls to ensure compliance to gas standards and regulations
- Alignment between the BANGS team and the Quality Management System (QMS) team to address recommendations resulting from the 2021 Lloyd's Register Group Limited (Lloyds Register) audit review of ISO 9001 compliance to maintain ISO 9001 certification
- Raw material procurement and testing activities
- Fabricated-component quality control testing activities
- BANGS order accounting and billing procedures
- Health and safety practices in place during the Internal Audit team's site visit to BANGS
- The appropriateness of users' access to key Information Technology (IT) applications used by BANGS employees

Internal Audit Finding Ratings

We assign ratings to audit findings based on the following scale (see the Internal Audit Finding Rating Scale in Appendix A):

"1" – Significant Improvement is Needed and Prompt Management Attention is Required

"2" – Improvement is Needed and Management Attention is Necessary

"3" – Some Improvement is Needed and Management Attention is Justified

"4" – Management Evaluation is Desirable

Internal Audit Conclusion and Summary of Observations

During the course of our review, we found that BANGS personnel are dedicated to continuous improvement and to consistently providing products and services that meet customer and regulatory requirements. The BANGS team is continuing to address recommendations communicated during the Lloyds Register ISO 9001 review, and the NiSource QMS team is working closely with the BANGS team to ensure BANGS is prepared for future audits and maintains processes consistent with ISO 9001 certification. During the Internal Audit team's visit to the BANGS facility, we also observed that BANGS personnel are committed to maintaining a safe and healthy work environment and following best practices.

Overall, process and controls related to the areas tested (as specified in the "Audit Objective, Approach, and Coverage" section of this report) were generally operating as intended, and we did not identify any notable findings. Less-significant items and recommendations to further improve processes and controls were discussed with management during the audit.

Management's Response

As we did not identify any notable findings, a management response was not requested.

Internal Audit Follow Up

Internal Audit follow up activities are not required related to this audit. We will evaluate the adequacy, effectiveness, and efficiency of controls associated with BANGS activities during the next Internal Audit of these processes.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Report *****

"1" Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company's reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

"2" Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

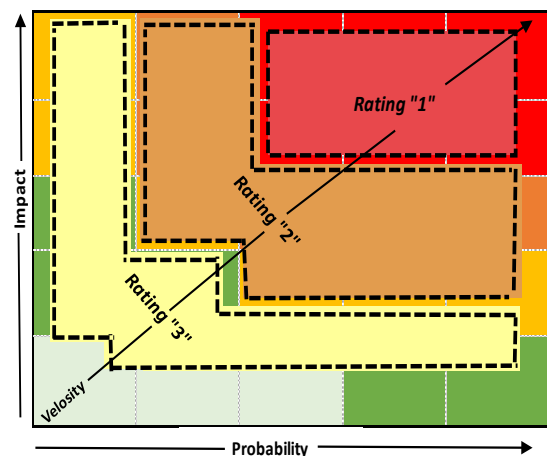
- More than remote probability for damage to the Company's reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls related are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

"3" Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

"4" Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited





SECURITY BASELINES

Advisory Review

January 2022

Distribution

Respondents

Carla Donev
Gregory Skinner

Beneficiaries

Tim Tokish

Other Key Personnel

Kimberly Jones
Daniel King
Austin Mitchell
Kevin Morris
Katy Perez
Ishreth Sameem

For Information

Shawn Anderson
Donald Brown
Kimberly Cuccia
Joseph Hamrock
Charles Shafer
Violet Sistovaris
Pablo Vegas



Big Thinking. Personal Focus.

This report has been prepared for use by NiSource management only, and is not to be distributed outside NiSource without permission from Schneider Downs & Co., Inc.

Table of Contents

Table of Contents 1

Executive Summary..... 2

 Background 2

 Current State..... 2

 Assessment Methodology..... 3

 Overall Risk..... 3

 Key Observations and Recommendations 4

 Management Response to Recommendations..... 6

Detailed Report 7

 Plan 8

 Build 11

 Run 13

Appendix A: Process Overview 16

Executive Summary

The services of Schneider Downs & Co, Inc. (Schneider Downs) were retained by NiSource Inc. (NiSource or the company) to perform an advisory review of key cybersecurity initiatives and provide a secondary opinion on the current-state design, and where applicable, operating effectiveness of NiSource's security baselining processes. NiSource Internal Audit selected security baselines for analysis based on its criticality related to the organization's cybersecurity posture, coupled with the program's maturity status within the broader NiSource cybersecurity roadmap. Schneider Downs' assessment occurred from June through October 2021.

For the purpose of this review, *security baselining* processes include:

- Adoption of standard configuration settings and operational attributes (collectively a *security baseline*) designed to improve the security posture for a specified component of IT architecture (e.g., operating system, enterprise application, networking equipment, database management system, etc.)
- Automated or manual processes used to deploy and maintain the adopted security baseline
- Risk assessment and monitoring of intentional and unintentional deviations from the security baseline
- Remediation of deviations and updates to system configurations in order to maintain compliance with successive versions of the security baseline

Background

NiSource's Information Technology function (NiSource IT) has historically developed technical specifications (known colloquially as *tech specs*) for major releases of production operating systems (OS) and enterprise software applications. These tech specs incorporate a combination of manufacturer recommendations, industry best practices, and organizational requirements into a single baseline configuration for the specified OS or application. While the development of tech specs includes multiple stakeholder groups within NiSource IT, both the deployment of new systems and reporting on the compliance of deployed systems aligned with established tech specs are the responsibility of NiSource's IT service provider, Tata Consultancy Services (TCS).

Current State

The configuration benchmarks provided by the Center for Internet Security (CIS Benchmarks) are the primary reference point utilized in the creation of new NiSource tech specs. The recommended configuration settings for each CIS Benchmark are exported from the Policy Compliance module within NiSource's Qualys vulnerability management scanning tool and reviewed by stakeholders in NiSource IT. Configuration settings with a known business justification for deviating from the "Recommended Value" in the CIS Benchmark are documented as "Agreed to Values". All such deviations are approved by appropriate representatives from NiSource IT's Engineering, Security, and Management functions, as well as subject matter experts (SMEs) from TCS. Tech specs are published and maintained during the service life of a given OS or enterprise application and retired when each product is phased out of service.

TCS is responsible for the implementation of systems in accordance with NiSource tech specs and for reporting on the compliance of deployed systems. While tech specs are applied to all Active Directory

(AD) domains established by NiSource and managed by TCS, compliance testing is currently performed for only one domain (the primary “NA” domain) of the fourteen domains. Of the total 3,054 assets tracked in NiSource IT’s ServiceNow configuration management database (CMDB) that were marked as being a production server device, slightly more than seventy percent (2,165 systems) were found to be covered by a current, non-archived technical specification. For the purposes of this review, endpoint devices were excluded from our analysis as they are not currently covered by the same processes as server devices. We recommend a separate review of endpoint security configurations due to the inherent risk involved with end-user computing.

Currently NiSource IT only requests tech spec compliance reports for a subset of systems and configuration settings deemed in-scope for Sarbanes-Oxley Act (SOX) controls testing and performs no review of systems outside of the scope of SOX testing. Because the SOX controls do not rely on all configuration settings in a given tech spec, less than half of the configuration settings enumerated in each tech spec are reviewed as part of SOX control testing efforts. Although the NiSource Information Security Controls Document (ISCD) requires IT service providers to perform tech spec compliance checking and remediation for all systems on at least an annual basis, we were unable to identify and verify formal compliance reporting or reviews performed over deployed non-SOX systems. Comprehensive compliance reporting is an in-flight initiative utilizing the Qualys Policy Compliance module, but we were unable to obtain a clear definition of how responsibilities for the ongoing maintenance of the platform would be owned between NiSource IT and TCS.

Assessment Methodology

A set of assessment objectives were established with input from members of the NiSource IT Governance, Risk, and Compliance (IT GRC) team. These objectives, along with corresponding observations and recommendations, are described in the following sections of this report.

For reporting purposes, activities assessed during this review were assigned to one of the three phases of the *Plan-Build-Run* model for IT infrastructure management. Use of this model from a reporting perspective is not a commentary or recommendation on its use by NiSource IT. For reference, a description of each phase in the *Plan-Build-Run* model is provided below with observations and recommendations for each phase found in the breakout pages that follow. A full process flow diagram for security baselining can be located in Appendix A: Process Overview.

Overall Risk



Because we were unable to obtain a reliable measure of compliance with published technical specifications, we cannot opine on the residual risk presented to NiSource that is due to non-compliant system configurations. Thus, the observations in this report are ranked according to the maximum potential risk that may either be introduced or undetected due to the identified process gap. Because

we observed approximately seventy percent of NiSource IT server assets are covered by a published technical specification and were unable to obtain any dedicated standard reporting process for measuring compliance with technical specifications, we have assessed the residual risk related to the security baselining processes to be 'High'. Specific observations and recommendations are enumerated below.

Key Observations and Recommendations

During this assessment, we noted that "tolerance stacking", the compounding of gaps at several subsequent stages of the process, creates a cumulative blind spot into the potential risk of non-compliance with accepted security baselines. These gaps are summarized below.

Observation #	1	Risk Ranking	High
Overview	Although Section 3.1 of the NiSource Information Security Controls Document (ISCD) requires IT service providers to perform tech spec compliance checking and remediation for all systems on at least an annual basis, we were unable to identify and verify formal compliance reporting or reviews performed over deployed non-SOX systems. NiSource systems being reviewed as part of SOX controls testing are being assessed for less than half of the configuration settings covered in the full tech spec.		
Risk	Because there is no dedicated process for assessing compliance with the established tech specs, the overall risk that non-compliant systems exist on the NiSource network is high. Non-compliant systems may expose the NiSource network to a level of risk unacceptable to NiSource management.		
Suggested Process Improvement	We recommend NiSource establish a standard process for reporting on the level of compliance to tech specs. As part of this process, we recommend NiSource IT management and TCS leadership align to define an automated tooling path (e.g., CIS-CAT Pro, Qualys Policy Compliance, etc.) for generating compliance metrics. Individual non-compliant systems should be flagged for remediation, and both non-compliance and policy exceptions should be handled through NiSource's existing IT risk management process.		
Management Response	IT Management will work with TCS to develop reporting on tech spec compliance for all assets, not just SOX assets (using Qualys or another tool). It is our understanding that all assets are built to tech specs but agree TCS currently does not demonstrate that compliance or have a process in place to flag items for remediation. We expect this process to be in place by the end of Q3 2022. (Ishreth/JoAnn)		

Observation #	2	Risk Ranking	Moderate
Overview	The current technical specification library covers approximately seventy percent of the IT server assets tracked in NiSource's ServiceNow configuration management database (CMDB).		
Risk	A significant number of currently deployed servers are either not covered by a tech spec or covered by a retired tech spec (indicating IT assets that should have been retired based on NiSource standards).		
Suggested Process Improvement	We recommend technical specifications be developed and maintained for all server assets across all domains within NiSource's IT environment. We further recommend NiSource regularly review the coverage of its current tech spec library against the IT asset inventory within the ServiceNow CMDB. Tech specs should only be retired when all covered systems have been removed from service, while systems without an applicable tech spec should be risk-rated and prioritized for the development of a tech spec.		
Management Response	IT Management currently develops tech specs based on demand and an ongoing 18-month rotation cycle. It is our understanding that TCS uses tech specs to build all server operating systems/databases in all NiSource domains. GRC will use the detailed data available from this review to assess opportunities for additional coverage and incorporate them into the review process. We will also review our internal process and assess if it can be more comprehensive. We will also look at end user devices and assess if tech specs are needed or if processes in place ensure appropriate security settings in the device configurations. A target date for a plan/approach is April 30, 2022, but we will likely have resource/budget impact requiring Management approval. (Kimberly/Kevin/Maurice)		

Observation #	3	Risk Ranking	Moderate
Overview	Because the Qualys Policy Compliance module only includes the attributes from CIS Benchmarks measurable by Qualys, using exports from this tool as input to the tech spec design process results in the exclusion of some recommended attributes from consideration during the development of new tech specs. We assessed between 17% and 56% of the total recommended attributes were missing from tech specs for the three most affected operating systems in NiSource's production environment (Windows Server 2016, VMWare ESXi 6.7, and Red Hat Enterprise Linux 7).		
Risk	The risk of excluding individual attributes depends on a variety of factors such as the nature of the attribute, exploitability of the alternate configuration, and any compensating attributes. The risk of excluding many attributes within a single tech spec greatly increases the likelihood that systems built to that configuration will be vulnerable to cyber-attack.		

Suggested Process Improvement	We recommend NiSource consider utilizing the CIS Benchmark documentation, either in its freely available PDF format, or the Excel format available to CIS Member organizations, instead of exports from the Qualys platform as the starting point for future tech spec design. We also recommend that exceptions to the baseline settings outlined in the CIS Benchmark be documented and reviewed regularly to determine if broad dependencies are impacting multiple tech spec families (e.g., if password settings frequently deviate from the CIS recommendation this may indicate a need to modify the organization-wide password configuration).
Management Response	IT Management will assess if greater coverage can be achieved using the current toolset available (Qualys) or if incremental budget is needed. Assets today are built to tech spec requirements and the response to Observation #1 should provide greater assurance relative to compliance. A target date for a plan/approach is June 30, 2022. If additional tooling is required, we may need to defer until 2023. (Kimberly/Kevin/Maurice)

Management Response to Recommendations

IT Management agrees with the observations noted by Schneider Downs and appreciates the review team providing process improvement recommendations. While Internal Audit does not formally track management action plans associated with advisory Internal Audit reviews, we have developed actions plans and target completion dates for each of the observations noted by Schneider Downs (which are documented above) and the IT GRC team will track progress of these action plans through completion.

*** End of Executive Summary ***

Detailed Report

Plan

Description & Assessment Objectives

The Plan phase encompasses the activities that result in an agreed-upon set of technical requirements that will be implemented as part of each technical specification (“tech spec”).

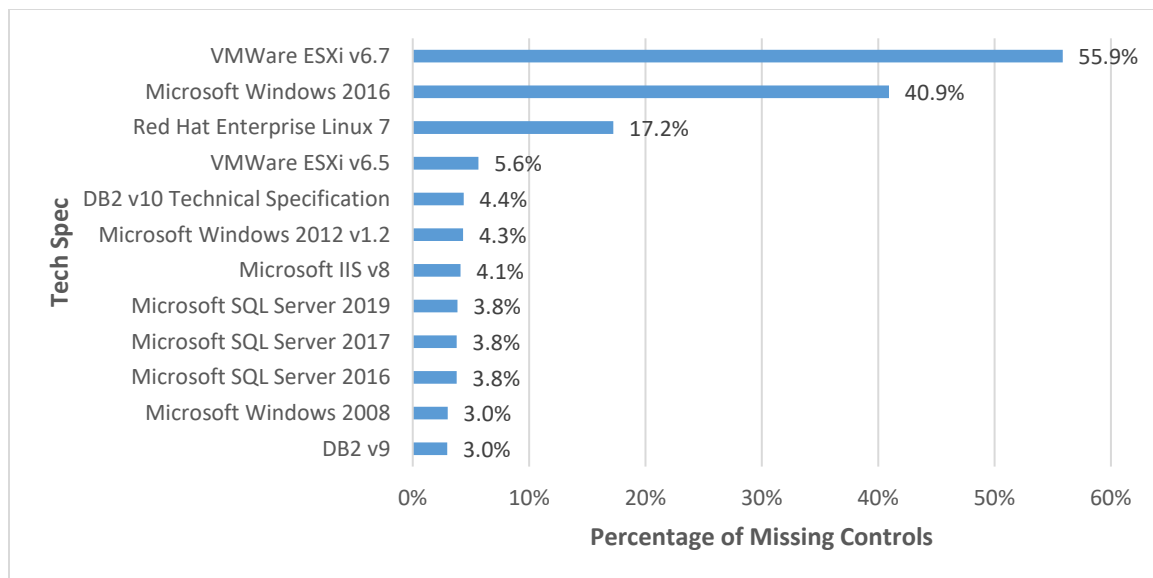
Objective	Description
2.1	Evaluate the documented tech spec for each system configuration against the standard attribute set defined in the corresponding CIS Benchmark.
2.2	Assess the completeness of coverage of corporate IT assets by existing tech specs, and the risk of assets currently unaddressed by a tech spec.

Recommendations

Objective	Observations and Recommendations
2.1	We observed several undocumented variances between sample technical specifications and the corresponding CIS Benchmark(s). We recommend utilizing official documentation from CIS or the software vendor as a starting point for all technical specifications instead of relying on the export feature from Qualys.
2.2	We were able to map less than seven percent of deployed systems to a current technical specification, indicative of several possible underlying issues: 1) end-of-life systems that have not been decommissioned, 2) operating systems and applications which are still under support by their manufacturers yet do not have a technical specification defined, and/or 3) system configuration data within the CMDB is incomplete or inaccurate. Schneider Downs recommends regular inventory reviews to ensure that all deployed systems are covered by one or more technical specifications.

Observations

Schneider Downs obtained the complete listing of seventy-five NiSource technical specifications used currently for production systems and selected a sample of twenty-five for testing. The twenty-five sample technical specifications were tested against the corresponding CIS Benchmark to identify the percentage of CIS Benchmark attributes missing from technical specification and the percentage of technical specification attributes that do not meet CIS Benchmark minimum recommendation. Thirteen of the sampled technical specifications were observed to have either greater than 3% deviation from the corresponding CIS Benchmark due to either missing attributes or attributes adopted with configurations weaker than the minimum recommendation, or both.



The chart above shows the twelve technical specifications that represent the highest risk areas for CIS Benchmark attributes missing from the technical specification. The three highest risk areas are: VMWare ESXi v6.7 with its technical specification missing 55.9% of the total CIS Benchmark attributes, followed by Microsoft Windows 2016 (40.9%) and Red Hat Enterprise Linux 7 (17.2%).

The VMWare ESXi v6.7 technical specification is missing sixty-two CIS Benchmark recommendations for settings related to:

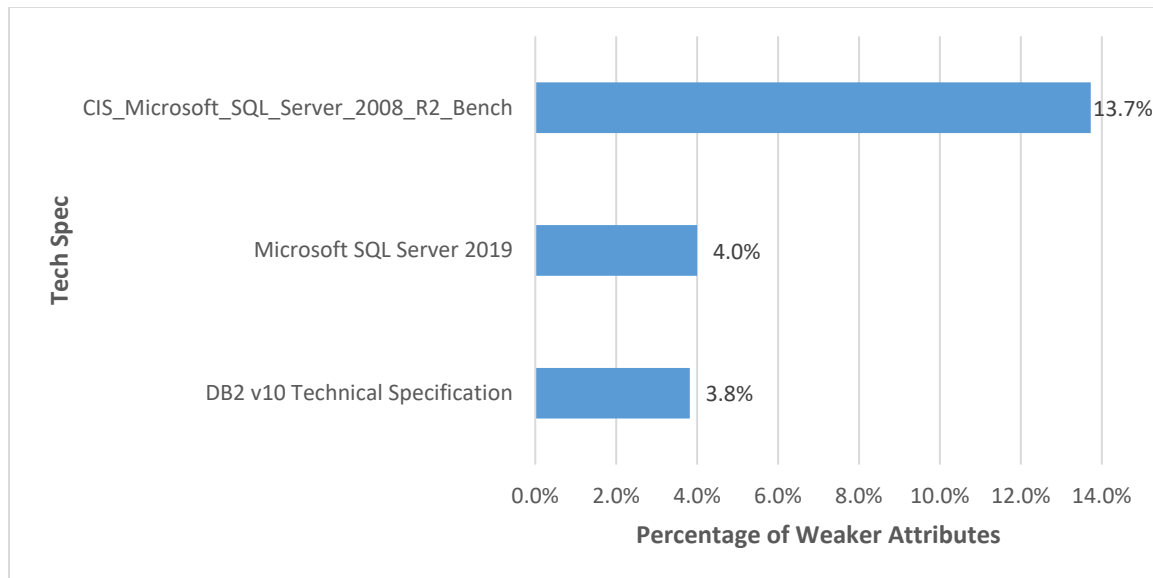
- Virtual machines (Section 8)
- vNetwork (Section 7)
- Communication (Section 2)

The Microsoft Windows 2016 technical specification is missing 149 CIS Benchmark recommendations for settings related to:

- Local policies (Section 2)
- Administrative Templates (Section 18)
- Advanced Audit Policy Configuration (Section 17)

The Red Hat Enterprise Linux 7 technical specification is missing 110 CIS Benchmark recommendations for settings related to:

- Initial Setup (Section 1)
- Network Configuration (Section 3)
- Access, Authentication, and Authorization (Section 5)



The chart above shows the three technical specifications that represent the highest risk areas based on the percentage of technical specification attributes that do not meet the CIS Benchmark minimum recommendation. The CIS_Microsoft_SQL_Server_2008_R2_Bench technical specification had 13.7% of attributes that did not meet the CIS Benchmark minimum recommendations followed by Microsoft SQL Server 2019 (4.0%) and DB2 v10 Technical Specification (3.8%). The latter two technical specifications both appear in the previous listing of technical specifications with many missing attributes.

The CIS_Microsoft_SQL_Server_2008_R2_Bench technical specification had attributes that do not meet CIS Benchmark minimum recommendations primarily for settings related to:

- Surface Area Reduction (Section 2)
- Authentication and Authorization (Section 3)
- Auditing and Logging (Section 5)

The Microsoft SQL Server 2019 technical specification had attributes that do not meet CIS Benchmark minimum recommendations primarily for settings related to:

- Surface Area Reduction (Section 2)
- Authentication and Authorization (Section 3)

The DB2 v10 technical specification had attributes that do not meet CIS Benchmark minimum recommendations primarily for settings related to:

- DB2 Configurations (Section 3)

The root cause of the identified variance between CIS Benchmarks and adopted NiSource technical specifications appears to be due to the inability of Qualys to scan for all attributes specified in each CIS Benchmark. Because Qualys cannot scan for all attributes, the Qualys exports used as a starting point for technical specifications are missing the attributes that Qualys does not have the ability to scan.

Build

Description & Assessment Objectives

The Build phase includes activities that support the design and implementation of the management technologies (such as Microsoft Active Directory) and individual systems in accordance with the established tech spec.

Objective	Description
2.3	Review the process(es) for configuring new systems and testing those configurations prior to production deployment.
2.4	Interview key stakeholders to determine whether all responsible parties have been trained appropriately on the procedures required for their roles.
2.5	For a sample of recently deployed systems (systems deployed after the publish date of the current version of a given tech spec), ensure that all deployment processes were followed and appropriately documented.

Recommendations

Objective	Observations and Recommendations
2.3	Through inquiry, we established new systems are built from a “golden image” that is designed in accordance with the NiSource tech spec, and that additional system settings are enforced using tools such as Microsoft Active Directory Group Policy Objects (GPOs). Each system is also configured using a build checklist which is attached to its system change records within the CMDB.
2.4	We noted through inquiry with key stakeholders that each group demonstrated knowledge of the procedures regarding technical specifications. However, the IT service provider (TCS) was unable to produce reliable/timely documentation of the current configurations for sampled systems as compared to relevant technical specifications. We recognize that NiSource has recently changed IT service providers and recommend the company establish standardized system compliance reporting with defined technical specifications, along with having the reporting be provided in alignment with contractual standards.
2.5	This objective was removed from our advisory scope to focus on objectives more directly related to the security baselining process.

Observations

We interviewed key stakeholders to understand the process used for configuring new systems and testing those configurations prior to production deployment. While the NiSource stakeholders are performing responsibilities consistent with their roles, there is a gap in the understanding of responsibilities regarding testing of pre-deployment scans.

Development of new technical specifications is triggered through one of two possible processes:

1. Projects are presented to the NiSource IT GRC team who then evaluate the project to identify whether the project contains systems that do not have a technical specification in place.

2. IT Infrastructure Engineering also informs IT GRC when a technical specification needs to be written.

Following the IT Policy Management Procedure, IT GRC will map the architect's information with the criteria and start the creation process. To facilitate creation of the technical specification, IT Security will export the CIS Benchmark scan settings from Qualys. IT GRC then reviews the CIS Benchmark export with input from IT Security and IT Infrastructure Engineering to establish the final technical specification which is to be approved and adopted.

NiSource uses a combination of vendor best practices and CIS Benchmarks in order to finalize its internal technical specifications. IT Security provides input to determine if a setting should be stronger than the CIS Benchmarks. IT Engineering validates that the system will function according to service levels with the technical specification settings in place. IT Infrastructure helps to provide support if there are questions and provide reasoning behind the configurations. For any setting that varies from the "Agreed to Value" in the CIS Benchmark, the SME and management document and approve the variance. If there are operating system or application settings that cannot meet the approved technical specification for a SOX system, an exception is opened in the SOX exception database owned by IT GRC and operated by the TCS compliance focal. No similar process exists for aggregating overall risk due to accepted variance between accepted configuration settings and the CIS recommendations.

A Technical Solution Document (TSD) is used for new solutions. Once the solution is handed over to IT Infrastructure, the TSD is reviewed to understand what should be built. IT Infrastructure does not validate the tech spec or the design of the solution in any way. IT Infrastructure expects that the solution was validated against the tech spec prior to being handed over.

Before infrastructure is deployed to production, it is validated against the technical specification. Once a technical specification is published in the library, all systems have a 90-day grace period from the published date in which to be compliant with the revised settings. If a technical specification is refreshed, the 90-day period starts over. While NiSource IT has a system build process in place, defined procedures are not in place regarding the pre-deployment technical specification review and validation process.

Run

Description & Assessment Objectives

The Run phases includes the activities performed for compliance monitoring and remediation of variances from the established tech specs.

Objective	Description
3.1	For samples of recently deployed systems, systems deployed prior to the publish date of the current tech spec and known legacy systems (systems known to be out of support by their vendor), identify the risk related to any variance between the system configuration and the corresponding tech spec coupled with how that risk is captured and ultimately mitigated or approved as-is.
3.2	Assess the tools and/or reporting available to NiSource IT in order to evaluate the compliance of corporate systems with established tech specs.
3.3	Review all items in the IT risk register related to configuration management to determine whether risks due to configuration variance are being appropriately reported to management.

Recommendations

Objective	Observations and Recommendations
3.1	We were unable to obtain reliable configuration data for deployed systems in order to complete this objective.
3.2	Due to the challenges described regarding Objective 3.1, we recommend utilizing a standard tool such as the CIS-CAT or the Qualys Policy Compliance module to create system-agnostic compliance reports.
3.3	We reviewed the risk management process around compliance testing for SOX-related systems. While this process appears to be operating effectively, coverage does not extend to all systems covered by one or more technical specifications. We recommend NiSource implement a similar compliance testing and remediation process for all such systems.

Observations

We determined NiSource does not currently perform technical specification compliance testing for non-SOX systems. We reviewed the technical specifications library, in-scope SOX system listing, and latest round of SOX testing and determine the following results.

	OS	Application	Total
Technical Specifications	28	47	75
In-Scope for SOX	6	0	6
Tested for SOX	4	0	4

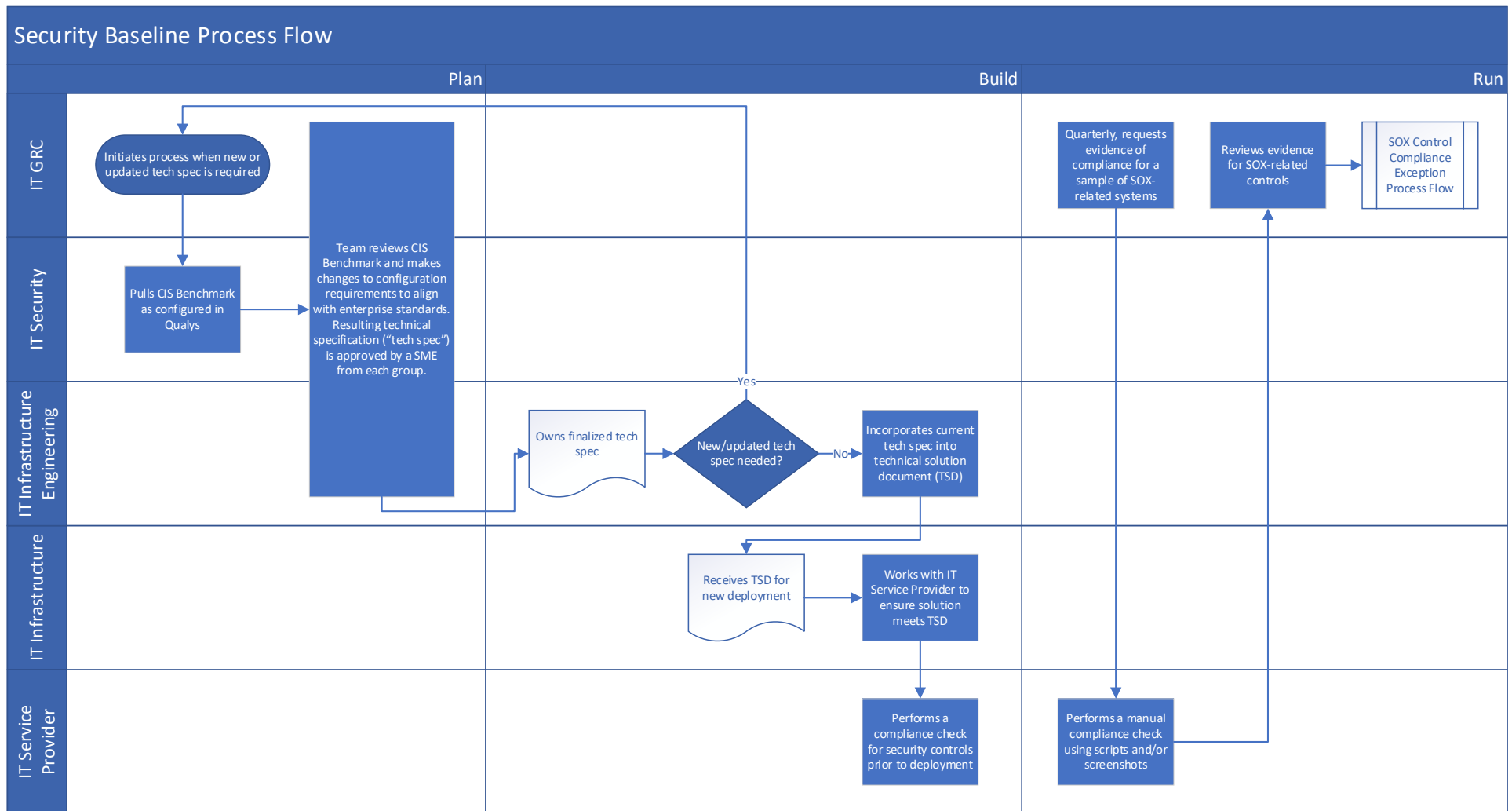
Based on the results above, sixty-nine technical specifications are not in scope for compliance testing and seventy-one were not tested based on the latest SOX sample selections. Additionally, we reviewed a total of eleven, randomly selected SOX servers for testing and determined nine out of the total eleven

SOX-related samples were tested using out-of-date technical specifications. Because we relied on variance in attribute numbering within a given tech spec to identify when a prior revision had been used for SOX testing, we were unable to ascertain if the two remaining systems sampled (Mainframes RED and BLUE) were tested using outdated tech specs as the attribute numbering was still aligned with the current tech spec. While the tech spec revision used to test each system was not documented, the test plan used during SOX testing was last revised in April 2016.

3Q2020 SOX Testing Samples	Tech Spec Attributes Tested for SOX	Total Attributes in Current Tech Spec Revision	Tech Spec Testing Coverage
Mainframe: RED zOS	22	483	4.55%
Mainframe: BLUE zOS	22	483	4.55%
VNXHAMAPEPMP01B PeopleSoft EPM / Datawarehouse NiFIT AIX	17	314	5.41%
VNXHAMAPWBLP01C PeopleSoft EPM / Datawarehouse NiFIT AIX	17	314	5.41%
VNXHAMCLPSFP02 PeopleSoft Financials NiFIT 9.1 AIX	17	314	5.41%
SWNHAMAPCSFP01B CIS WIN2K8	55	420	13.10%
OWNCNAP0012 NA Domain Controller WIN2K12	56	420	13.33%
OWNHAMPO069 Intense WIN2K12	56	420	13.33%
PVWIHAMWAAPG00 Corptax WIN2K12	56	420	13.33%
VWNHAMAPEPMP14 Hyperion Financial Mgmt WIN2K12	56	420	13.33%
VWNHAMDBSQLP25B iNovah WIN2K12	56	420	13.33%

While none of the attributes tested were out of scope when compared against the current revision of tech specs, we were unable to assert their compliance with the most recent revisions of the corresponding tech spec. The table above details the number of attributes tested as part of SOX testing procedures, the total number of attributes in the current revision of tech specs, and the overall testing coverage provided through SOX testing.

Appendix A: Process Overview



NiSource Corporate Services Company

Environmental Function General Controls

Internal Audit Report

Distribution

Respondents

Kelly Carmichael

Beneficiaries

Brent Archer

Kimra Cole
Mark Kempic
Vincent Parisi

Michael Hooper

Other Key Personnel

Stephen Holcomb

Brian Kortum
Marc Okin
Maureen Turman

Johnnie Long

For Information

Shawn Anderson
Donald Brown
Kimberly Cuccia
Charles Shafer
Violet Sistovaris
Pablo Vegas
Lloyd Yates

Internal Audit Report

Background

NiSource Inc. (NiSource or the Company) is committed to delivering energy safely, reliably and in an environmentally responsible and sustainable way, in accordance with federal, state, and local environmental requirements. The Environmental function is responsible for: 1) overseeing and ensuring that all employees understand their role and responsibility for achieving environmental goals; 2) integrating and enhancing environmental considerations into all business activities; and 3) demonstrating and promoting pollution prevention, environmental preparedness, waste minimization and recycling.

NiSource has committed to a 90% reduction of greenhouse gas by 2030 – using the industry-standard baseline of 2005 as determined by the Paris climate agreement. In 2020, NiSource was named to the Dow Jones Sustainability North America Index for the seventh consecutive year. The Company's environmental reports provide investors with both quantitative and qualitative environmental and sustainability information, including environmental impact targets such as reduction in greenhouse gas, methane from mains and services and coal ash generated, in addition to NiSource's timeline to retire coal-fired generation facilities.

Audit Objective, Approach, and Coverage

The objective of this risk-based internal audit was to provide an independent evaluation of the adequacy, effectiveness and efficiency of controls associated with the Environmental function. At the beginning of our audit, we completed a risk assessment and we conducted detailed process assessments and sample-based transactional testing in higher-risk areas. The review period for this audit was January 1, 2020 through August 31, 2021.

During the audit, we specifically evaluated:

- Management of Environmental function policies and procedures, with focus on high-risk corporate and external policies such as the Climate Change and Environmental Health and Safety policies, including NiSource Gas and Electric Environmental Standards
- Environmental legislation change monitoring, evaluation and communication to stakeholders
- The design of environmental reporting processes and approach for calculating baseline (2005), current (2020) and projected (2030) data for the following metrics: greenhouse gas, nitrogen oxides, sulfur dioxide, mercury, water withdrawal, water discharge and coal ash generated
- Processes related to monitoring environmental permitting and compliance, with focus on tracking corrective actions on deviations
- Existence of a formal process for review of environmental reserve reporting

We did not evaluate the environmental asset retirement obligation and the emergency response plan which will be considered in future audits. Additionally, we did not evaluate the completeness and accuracy of data feeding into environmental reporting, which will also be covered in an audit planned to occur during 2022.

Internal Audit Finding Ratings

We assign ratings to audit findings based on the following scale (see the Internal Audit Finding Rating Scale in Appendix A):

"1" – Significant Improvement is Needed and Prompt Management Attention is Required

"2" – Improvement is Needed and Management Attention is Necessary

"3" – Some Improvement is Needed and Management Attention is Justified

"4" – Management Evaluation is Desirable

Internal Audit Conclusion and Summary of Observations

Environmental management recently enhanced procedures on environmental permitting processes for corrective actions on permitting deviations to promote consistency and alignment with legislative permitting requirements, which facilitated a 32% reduction in deviation rate from 2020 to 2021. In addition, the Environmental Compliance team introduced a facility self-assessment program in 2020, which enabled expanded assessment coverage and improved tracking and monitoring of deviation rates at a local level.

Overall, we found that processes and controls related to the areas tested (as specified in the “Audit Objective, Approach, and Coverage” section of this report) were generally operating as intended. We did, however, identify two findings where management’s attention is justified (Rating 3). In addition, we observed some less-significant opportunities for improvement that were discussed with management during the course of the audit.

A summary of audit findings rated “1” through “3” follows (see the Internal Audit Findings Matrix in Appendix B):

- 1) *Formalization of Controls Associated with Environmental Reporting* (Rating 3)
Procedures and controls associated with key environmental metrics and associated data collection, analysis, and compilation are not formally and comprehensively documented, which could result in inconsistency and impair validation activities.
- 2) *Monitoring Corrective Actions Remediation for Higher-Risk Environmental Compliance Deviations* (Rating 3)
Documentation evidencing that corrective actions related to high-risk deviations were appropriately remediated was not always obtained (which is required by policy). Also, the status of remediation actions was not always monitored through completion.

Management’s Response

Management agrees with the findings noted as a result of this audit and have provided action plans to address the risk identified. Detailed action plans are included in Appendix B. Management is committed to ensuring the accuracy and completeness of NiSource’s Environmental Social and Governance (ESG) reporting and disclosure by implementing the Workiva ESG reporting software solution to ensure auditability, transparency and traceability of ESG data. The implementation will be completed by September 1, 2022. Additionally, management will ensure that corrective actions for high-risks deviations identified in the Facility Self-Assessment program and Capital Construction Inspection Program are completed in a timely manner. All key mitigation plans will be completed by December 1, 2022.

Internal Audit Follow Up

Management has provided action plans for all findings with a rating of “1”, “2”, or “3”. We have reviewed management’s action plans and believe that the action plans will adequately address the findings identified in this audit. We will track the progress of resolution and will conduct follow-up testing for all rated “1” audit findings and a sample of rated “2” and rated “3” audit findings.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Report *****

"1" Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company's reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

"2" Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

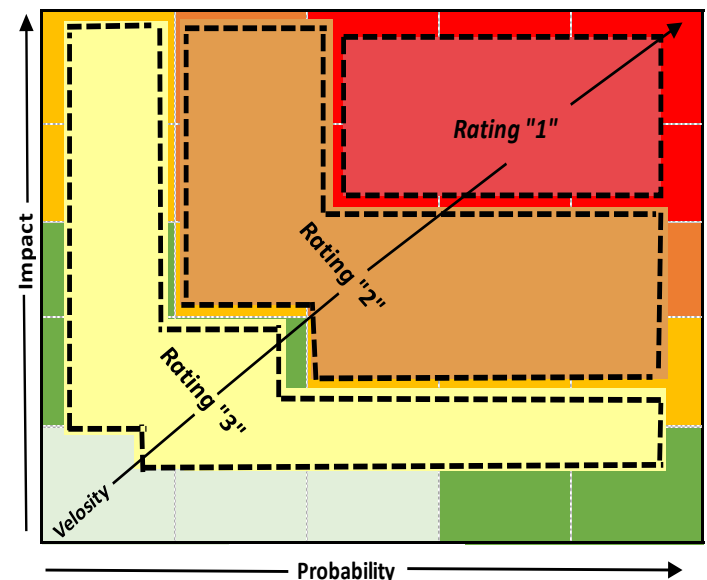
- More than remote probability for damage to the Company's reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls related are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

"3" Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

"4" – Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited



1) <u>Formalization of Controls Associated with Environmental Reporting</u>	<u>Rating: 3</u>
<u>Observation:</u> The NiSource Inc. (NiSource or the Company) Environmental team engaged Trinity Consultants, Inc. (Trinity) to independently validate and attest to greenhouse gas emissions and key performance indicators externally reported in 2020. Trinity's assurance assumes that the Company's data is sufficient, accurate and complete. However, procedures and controls associated with key environmental metrics and associated data collection, analysis and compilation are not formally and comprehensively documented, which could result in inconsistency and impair validation activities. <u>Criteria:</u> Processes related to calculating performance against targets for key environmental metrics related to greenhouse gases, nitrogen oxides, sulfur dioxide, mercury, water and coal ash are adequate to ensure that externally reported information is accurate; specifically: 1) performance metrics, including objectives and expected outcomes, are formally defined; 2) metric calculation methodologies, including key data required, are formally defined; 3) internal controls, including controls to ensure the completeness and accuracy of key data, have been designed, formally documented and are periodically tested; and 4) roles and responsibilities are formally defined. <u>Risk:</u> Insufficient process documentation for environmental metrics may result in data reported externally being inaccurate and/or misleading, resulting in a negative impact to the Company's reputation.	<u>Management Action Plan:</u> We commit to formally defining NiSource's critical environmental metrics. Each definition will include objectives, expected outcomes, calculation methodology and key underlying data requirements. We are implementing a new software solution, Workiva Environmental, Social and Governance (ESG) reporting, that is similar to the solution that NiSource uses for Securities and Exchange Commission (SEC) and Federal Energy Regulatory Commission (FERC) reporting. Workiva ESG reporting is a platform to collect and record ESG data in one system. Workiva also contains NiSource's ESG reporting and disclosure templates, which will be mapped to the underlying ESG data that has been collected. This process will ensure the completeness and accuracy of data and the associated downstream reports and disclosures. This connected nature of the data and reports will promote auditability, transparency and traceability. Finally, Workiva's administrative and permission controls allow for customized, scheduled follow-up to internal data providers and reviewers. This ensures that roles and responsibilities are formally defined. The Program Manager will ensure implementation of this management action plan. <u>Responsible:</u> Kelly Carmichael, VP Federal Government Affairs, Environmental and Sustainability <u>Resolution Date:</u> 9/1/2022

2) <u>Monitoring Corrective Actions Remediation for Higher-Risk Environmental Compliance Deviations</u>	<u>Rating:</u> 3
<u>Observation:</u> The Environmental Compliance group oversees the execution of self-assessment audits of NiSource facilities, including documentation of environmental deviations noted during the audits, which are categorized by risk. Documentation evidencing that corrective actions related to high-risk deviations were appropriately remediated was not always obtained (which is required by policy). Also, the status of remediation actions was not always monitored through completion. As a result, we could not validate that all high-risk deviations were remediated timely. <u>Criteria:</u> A framework for monitoring corrective actions for high-risk Environmental Compliance deviations at NiSource facilities should be established; specifically, ensure actions taken are: 1) in compliance with regulatory requirements; 2) completed timely based on urgency of risk and available resources; and 3) documented and retained centrally as evidence of environmental quality and compliance. <u>Risk:</u> High risk deviations identified in self-assessments are not corrected, leading to citations, fines or reputational harm to NiSource.	<u>Management Action Plan:</u> We will establish a risk-based process to differentiate environmental deviations identified through the facility self-assessment (FSA) program, as well as deviations identified through the capital construction inspection program. A deviation, as defined for both programs, is as follows: an infraction of federal, state or local agency environmental permit requirements, conditions, laws or regulations which could result in an enforcement action; a failure to follow NiSource environmental standards, policies and procedures; or a corrective action that has not been completed within the required time frame. High-risk deviations will be distinguished from low-risk deviations based on the potential to result in an enforcement action and will be reviewed to ensure proper corrective actions are completed in a timely manner. Appropriate documentation for each high-risk deviation will be maintained as part of the respective programs and will be available for periodic reviews and audits. The Director of Environmental Compliance will ensure the implementation of the management action plan with respect to the FAS Program. The Director of Environmental Permitting will ensure the implementation of the management action plan with respect to the Capital Construction Inspection Program. <u>Responsible:</u> Kelly Carmichael, VP Federal Government Affairs, Environmental and Sustainability <u>Resolution Date:</u> 12/1/2022

3) <u>Periodic Review of Environmental Policy and Procedure</u>	<u>Rating: 4</u>
<u>Observation:</u> A formal process to periodically review key environmental policies is not established. However, at the time of our audit, we found that NiSource's Environmental policy and procedure documents, including Environmental Gas Standards and NIPSCO Generation Environmental Electric Orders, covered a comprehensive span of topics. <u>Criteria:</u> A formal process is established to review key policies and procedures; specifically: 1) management maintains an inventory of all policies and procedures; 2) policies and procedures are periodically reviewed on a risk basis; 3) as applicable, policies and procedures are updated; and 4) key policy and procedure changes are communicated to relevant business partners. <u>Risk:</u> Potential that policies, procedures, standards and general orders specific to the Environmental function are not consistently executed in conformance with legislative and company requirements if policy and procedure documents are outdated or not appropriately communicated.	<u>Management Action Plan:</u> An operational objective has been developed as part of the Environmental Policy & Sustainability 2022 business plan to enhance various programs within the Environmental Management System, including a project to modernize and improve environmental protocol, process, procedure and policy documentation management and information communication processes. The project will bring together a cross functional team of representatives from each team within the Environmental function to create a more effective control framework. Ultimately, once the framework is in place for documents controlled by the Environmental Policy & Sustainability Department, the standing team created to manage documentation on an ongoing basis will ensure coordination with other key areas that use/share environmental information, including Operations, Industrial Hygiene, Safety, Training, Human Resources and Change Management. The ultimate mission of the project is to define clear ownership and control of stand-alone and shared environmental documentation and to ensure that environmental information in all its forms is current, accurate and readily accessible when needed. The Manager of Environmental Management will ensure the implementation of the management action plan. <u>Responsible:</u> Kelly Carmichael, VP Federal Government Affairs, Environmental and Sustainability <u>Resolution Date:</u> 09/01/2022

4) <u>Environmental Compliance Task Tracking Mechanism</u>	<u>Rating:</u> 4
<u>Observation:</u> The Essential Task Manager Tracker is not monitored or reviewed to ensure that all Environmental tasks are completed on-time or that outdated tasks are removed from the tracking system. At the time of our audit, nine percent of tasks were overdue and 18% of tasks were completed late. Based on a review of the overdue and completed-late tasks, processes to ensure that higher-risk tasks are completed timely are appropriate; however, efficiency can be improved by further formalizing processes and removing outdated tasks from the tracking system. <u>Criteria:</u> Periodic reviews of the Essential Task Manager Tracker should be conducted by a designated administrator to ensure that the Environmental tasks housed within the system are current and outdated or obsolete tasks are cleared from the system to allow task owners to focus on relevant items. <u>Risk:</u> Inaccurate and obsolete information in the Essential Task Manager tool could impair processes to effectively and efficiently monitor completion of environmental tasks.	<u>Management Action Plan:</u> We will implement a process to periodically review items within the Essential Task Manager and update or remove outdated tasks. A task will be created within Essential to perform this review, with a recurrence pattern of once per quarter. The task will be configured to send an email reminder one week before the task due date, a second email on the due date and a final email the day following the due date if the task has not been completed. The Program Manager will ensure the implementation of the management action plan. <u>Responsible:</u> Kelly Carmichael, VP Federal Government Affairs, Environmental and Sustainability <u>Resolution Date:</u> 05/01/2022

***** End of Report*****

NiSource Corporate Services Company

Identity and Access Management (IAM) Execution

Internal Audit Report

Distribution

Respondents

Carla Donev
Kevin Johannsen

Beneficiaries

Michael Rosello Gregory Skinner Timothy Tokish

Other Key Personnel

Kimberly Jones Daniel King Kevin Morris
Quentin Walls

For Information

Shawn Anderson
Donald Brown
Kimberly Cuccia
Charles Shafer
Violet Sistovaris
Pablo Vegas
Lloyd Yates

Internal Audit Report

Background

In November of 2019, NiSource Inc. (NiSource or the Company) engaged Accenture plc (Accenture) to design and implement a modern Identity and Access Management (IAM) solution consisting of the SailPoint IdentityIQ, CyberArk Privileged Access Manager and Ping Identity applications. These solutions replaced NiSource's existing legacy IAM application stack of Hitachi ID Identity Manager, Hitachi IT Privileged Access Manager, IBM Security Access Manager and RSA. The technical IAM migration was performed by Accenture with NiSource Information Technology (IT) management providing internal guidance, requirements and ongoing project management support. The objectives of this migration were to:

- Build the base SailPoint infrastructure and implement foundational SailPoint user access provisioning capabilities
- Set up the base infrastructure and application structure for CyberArk Privileged Access Manager and Ping Identity for end user identification
- Operationalize a factory model to onboard additional applications and accounts for all three NiSource IAM applications

The cost of the IAM implementation project totaled \$10.5 million. In late 2020, upon conclusion of the project, management and governance of the new IAM solution was transitioned to an internal IAM support team within NiSource IT Security. This IAM support team is responsible for day-to-day management of the IAM tool suite.

Audit Objective, Approach, and Coverage

The objective of this risk-based audit was to provide an independent evaluation of the adequacy, effectiveness, and efficiency of processes and controls associated with supporting the new NiSource IAM application stack post-implementation. At the beginning of our audit, we completed a risk assessment, and we conducted detailed process assessments and transactional testing in the highest-risk areas. The review period for this audit was August 2021 through October 2021.

During the audit, we specifically evaluated:

- Processes and controls related to the management of business user access within SailPoint IdentityIQ, including controls around access entitlements
- Privileged access provisioning within CyberArk Privileged Access Manager, including adherence to corporate policies, assigning and approving privileged access and management/recertification of privileged accounts

We did not evaluate processes and controls over the Ping Identity application due to the comparatively lower risk profile of this end user identification tool. We also did not evaluate controls outside of the IAM tools mentioned above, such as network and system security configurations, application security configurations, etc.

Internal Audit Finding Ratings

We assign ratings to audit findings based on the following scale (see the Internal Audit Finding Rating Scale in Appendix A):

"1" – Significant Improvement is Needed and Prompt Management Attention is Required

"2" – Improvement is Needed and Management Attention is Necessary

"3" – Some Improvement is Needed and Management Attention is Justified

"4" – Management Evaluation is Desirable

Internal Audit Conclusion and Summary of Observations

During the course of our review, we noted the provisioning, review and removal of end user access has been simplified through the use of SailPoint IdentityIQ by providing a single application for NiSource business users and approvers to perform these user access functions. We also observed that NiSource's implementation of CyberArk Privileged Access Manager has provided the IAM support team with a robust and complete means of vaulting and securing accounts with privileged access within the NiSource computing environment.

Overall, post-implementation of the SailPoint and CyberArk applications, we found the process and controls related to the areas tested (as specified in the "Audit Objective, Approach, and Coverage" section of this report) were generally operating as intended. We did, however, identify one finding where management's attention is necessary (Rating 2) and one finding where management's attention is justified (Rating 3). In addition, we observed some less-significant improvement items that were discussed with management during the audit.

A summary of audit findings rated "1" through "3" follows (see the Internal Audit Findings Matrix in Appendix B):

- 1) *Inconsistency in Privileged Account Vaulting and Compliance with Password Policy Requirements* (Rating 2)
NiSource IT policy specifies that all privileged accounts should be identified and maintained in an account vaulting tool for adequate central control, tracking and password distribution purposes. However, not all privileged accounts are vaulted as required per policy. In addition, the IT team has identified approximately 5,000 application accounts that are not in compliance with password policy expiration requirements.
- 2) *Active Directory (AD) Group Entitlement Governance Processes* (Rating 3)
Some processes and activities related to governing Active Directory (AD) group entitlements are not formalized.

Management's Response

Management is aligned with Internal Audit's findings and will implement remediation approaches. Detailed action plans are included in Appendix B. The key mitigation steps and development of detailed risk-based remediation plans will be completed by April 2022.

While full implementation and execution of detailed risk-based remediation plans will continue into 2023, risk associated with privileged accounts that are not maintained within CyberArk and with accounts that are not in compliance with password policy expiration requirements is partially mitigated by other controls in place, including firewalls, security requirements to access the NiSource network, two-factor authentication for critical systems and security monitoring activities.

Internal Audit Follow Up

Management has provided action plans for all findings with a rating of "1", "2", or "3". We have reviewed management's action plans and believe that the action plans will adequately address the findings identified in this audit. We will track the progress of resolution and will conduct follow-up testing for all rated "1" audit findings and a sample of rated "2" and rated "3" audit findings.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Report *****

"1" Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company's reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

"2" Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

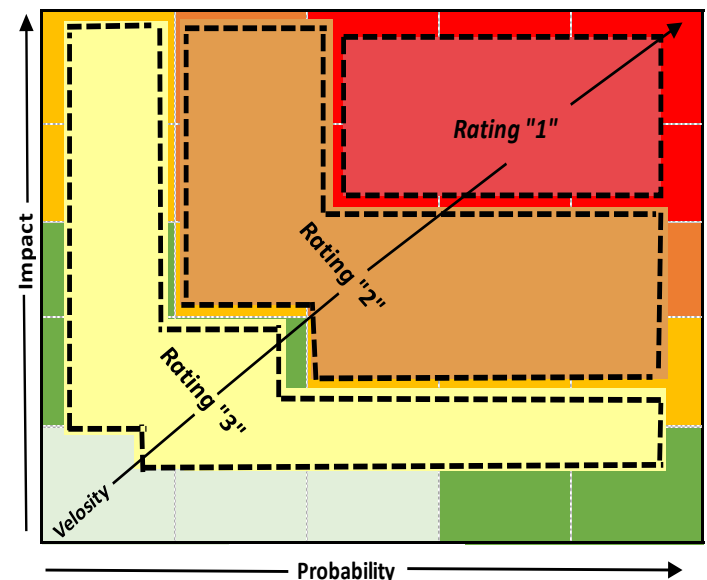
- More than remote probability for damage to the Company's reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls related are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

"3" Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

"4" – Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited



1) <u>Inconsistency in Privileged Account Vaulting and Compliance with Password Policy Requirements</u>	<u>Rating: 2</u>
<u>Observation:</u> NiSource Information Technology (IT) policy specifies that all privileged accounts should be identified and maintained in an account vaulting tool for adequate central control, tracking and password distribution purposes. However, at the time of our audit, not all privileged accounts are vaulted as required per policy. In addition, the IT team has identified approximately 5,000 application accounts that are not in compliance with password policy expiration requirements. <u>Criteria:</u> Controls are sufficient to ensure that all privileged accounts – i.e. accounts with elevated access - within the NiSource IT computing environment are vaulted within the CyberArk Privileged Manager access management tool to allow for enhanced security and monitoring. Also, account passwords are in compliance with password policy requirements. <u>Risk:</u> Potential that privileged accounts not vaulted within the CyberArk Privileged Manager tool can be utilized in an improper, unsupervised or unmonitored manner increasing the risk of inappropriate changes not being prevented or detected timely.	<u>Management Action Plan:</u> The risk associated with privileged accounts that are not maintained within CyberArk and with accounts that are not in compliance with password policy expiration requirements is partially mitigated by other controls in place, including firewalls, security requirements to access the NiSource network, two-factor authentication for critical systems and security monitoring activities. IT Management agrees that all privileged accounts need to be housed in CyberArk as either managed or vaulted accounts and also agrees that accounts not in compliance with password policy expiration requirements should be remediated. IT management will specifically: • Implement a process requiring all new service accounts and other privileged accounts to be loaded in CyberArk at creation (with required fields) • Create and execute a plan to cleanup existing privileged accounts; the plan will include steps to develop: 1) account assessment criteria, 2) account risk assessment process and 3) timelines for vaulting accounts, which will be based on account risk ratings and 4) required participation from Data Center, Applications, Network, and Security towers • Proceed with executing the plan to significantly reduce accounts with non-expiring passwords, including: 1) effective October 1, 2021, automatic renewal/acceptance of new non-expiring accounts was stopped, 2) requirements have been documented, 3) a formal project to remove the non-expiring flag has been initiated and the project plan is being finalized, including accounts being prioritized for remediation based on risk <u>Responsible:</u> Carla Donev, VP & Chief Information Security Officer (point) Kevin Johannsen, VP IT Application Services (support)

	<u>Resolution Date:</u> The new CyberArk processes for service/privileged accounts will be implemented by April 1, 2022. A plan to cleanup privileged accounts that are currently not vaulted will be developed by April 1, 2022; dates associated with specific action steps to be identified in the plan are to be determined. A formal project to address accounts not currently in compliance with password policy expiration requirements will be finalized by April 1, 2022; dates associated with specific action steps to be identified in the plan are to be determined.
2) <u>Active Directory (AD) Group Entitlement Governance Processes</u>	<u>Rating:</u> 3
<u>Observation:</u> Some processes and activities related to governing Active Directory (AD) group entitlements are not formalized. We specifically noted: - Standards defining how and when AD group entitlements should be applied are not formalized and current practices are inconsistent across IT groups - While enterprise naming standards have been established, some AD group entitlements do not follow the established standards and remediation expectations and plans are not established - Processes defining how AD group ownership is maintained and kept current, including the definition of key roles and responsibilities, are not established Training for personnel requesting, approving or certifying user access provisioned using AD group entitlements is not sufficient to ensure that user access requests, approvals and certifications are based upon sufficient knowledge and understanding of the associated access permissions.	<u>Management Action Plan:</u> As noted by Internal Audit, AD naming standards have been established. NiSource Identity and Access Management (IAM) will work with data center services to ensure all new groups adhere to these standards and members are only added through a SailPoint access request. IAM maintains group ownership as we are notified of changes. A certification of resource owners is on the 2022 roadmap and will complete by November 2022. Group ownership certification will be prioritized in the 2023 roadmap. (Carla/Quentin/Kevin/Katy – Quentin to drive) <u>Responsible:</u> Kevin Johannsen, VP IT Application Services (point) Carla Donev, VP & Chief Information Security Officer (support) Mike Rosello, VP Chief Enterprise Architect & IT Transformation (support) <u>Resolution Date:</u> Enforcement of new group alignment to naming standards will be emphasized with our IAM team and service provider effective immediately. We will also ensure members are only added via a SailPoint access request. Finally, we will coordinate with data center services to ensure alignment with these processes by April 1, 2022.

<u>Criteria:</u> Processes and controls are sufficient to promote efficient and effective user access management activities, specifically: 1) policies and standards are defined and documented; 2) policies and standards, including naming standards, are adhered to; 3) key roles and responsibilities are formally defined and understood; and 4) personnel responsible for requesting, approving or certifying access are sufficiently trained. <u>Risk:</u> Potential for inappropriate user access to be requested, approved, provisioned and not identified through access review activities, which could negatively impact data integrity or result in roles not being appropriately segregated within information technology applications.	Ongoing certification of key roles and membership will be accomplished using the SailPoint certification process. Resource owners will be certified by November 2022. Group member certifications will begin in January 2023 with a targeted completion by June 2023. Finally, there will be ongoing efforts to align existing groups to naming conventions.

***** End of Report*****

NiSource Inc.

Integration Center General Controls

Internal Audit Report

Distribution

Respondents

Lloyd Tiffner
Dan Williamson

Beneficiaries

Dan Douglas

For Information

Shawn Anderson
Donald Brown
Kim Cuccia
Charles Shafer
Violet Sistovaris
Pablo Vegas
Lloyd Yates

Internal Audit Report

Background

NiSource Inc. (NiSource or the Company) serves approximately 3.6 million gas and 470,000 electric customers across six states. The Integration Center (IC) is responsible for scheduling field activities, completing work preparation and closeout tasks, interfacing with customers, monitoring exceptions and compliance of work performed and dispatching crews to emergencies. Annually, the IC manages logistics for over 2,000 technicians executing approximately 2.5 million job orders, including responding to approximately 130,000 emergencies. The IC was engaged by Eversource Energy (Eversource) to provide support and training to Eversource employees after their purchase of Columbia Gas of Massachusetts during the period of October 2020 through March 2021.

The IC operates from two locations: one in Columbus, Ohio, which serves the five Columbia Distribution Companies (CDC), and one in Merrillville, Indiana, which serves Northern Indiana Public Service Company (NIPSCO) Gas and Electric. The IC structure is aligned by state to ensure the unique compliance and scheduling needs of each state can be addressed by knowledgeable personnel.

Audit Objective, Approach, and Coverage

The objective of this risk-based internal audit was to provide an independent evaluation of the adequacy, effectiveness and efficiency of controls associated with IC processes and activities performed to support the affiliated gas distribution companies. At the beginning of our audit, we completed a risk assessment, and we conducted detailed process assessments and sample-based transactional testing in higher-risk areas. The review period for this audit was January 1, 2021 through December 31, 2021.

During the audit, we specifically evaluated:

- Adherence to requirements of the Transition Service Agreement (TSA) between Eversource and NiSource
- Coordination with field personnel and associated compliance and customer interface activities
- Emergency response monitoring processes
- Scheduling processes and associated monitoring controls
- Job order preparation and close out processes
- User access controls specific to applications managed by the IC

IC processes and controls supporting NIPSCO Electric were not included in the scope of this review and will be evaluated during future audits.

Internal Audit Finding Ratings

We assign ratings to audit findings based on the following scale (see the Internal Audit Finding Rating Scale in Appendix A):

“1” – Significant Improvement is Needed and Prompt Management Attention is Required

“2” – Improvement is Needed and Management Attention is Necessary

“3” – Some Improvement is Needed and Management Attention is Justified

“4” – Management Evaluation is Desirable

Internal Audit Conclusion and Summary of Observations

The IC is appropriately structured to dynamically support field processes, and the IC team effectively executes scheduling activities to navigate unforeseen challenges and manage risk. Also, work plan monitoring activities, including metrics, enable the IC team to make necessary adjustments while ensuring execution targets are met and compliance activities are completed.

The IC is undertaking several initiatives to assess process consistency and enhance procedural documentation. As strong policies and procedures support consistency and knowledge transfer, we recommend continuing to focus on these efforts with particular attention on standardizing processes between the teams operating in Columbus and Merrillville where possible.

Overall, we found that processes and controls related to the areas tested (as specified in the “Audit Objective, Approach, and Coverage” section of this report) were generally operating as intended. We did, however, identify two findings where management’s attention is justified (Rating 3). In addition, we observed one less-significant item that was discussed with management during the audit.

A summary of audit findings rated “1” through “3” follows (see the Internal Audit Findings Matrix in Appendix B):

- 1) Controls Over Adjustments to NIPSCO Gas Emergency Response Exceptions (Rating 3)
IC personnel review, validate and frequently adjust exceptions to the emergency response time target prior to the delayed emergency response metric being calculated. Adjustments to NIPSCO Gas emergency response exceptions are not confirmed by a supervisor and documentation evidencing the reason for adjustments is not consistently retained.
- 2) IC Application Access Controls (Rating 3)
User access to specific data or functions within the IC applications is not periodically reviewed and verified to ensure that access is consistent with the users’ roles and responsibilities.

Management’s Response

We agree with the findings noted during this audit and have provided management action plans to address the risks identified in Appendix B. All action plans will be completed by October 2022.

Internal Audit Follow Up

Management has provided action plans for all findings with a rating of “1”, “2”, or “3”. We have reviewed management’s action plans and believe that the action plans will adequately address the findings identified in this audit. We will track the progress of resolution and will conduct follow-up testing for all rated “1” audit findings and a sample of rated “2” and rated “3” audit findings.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Report *****

"1" Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company's reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

"2" Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

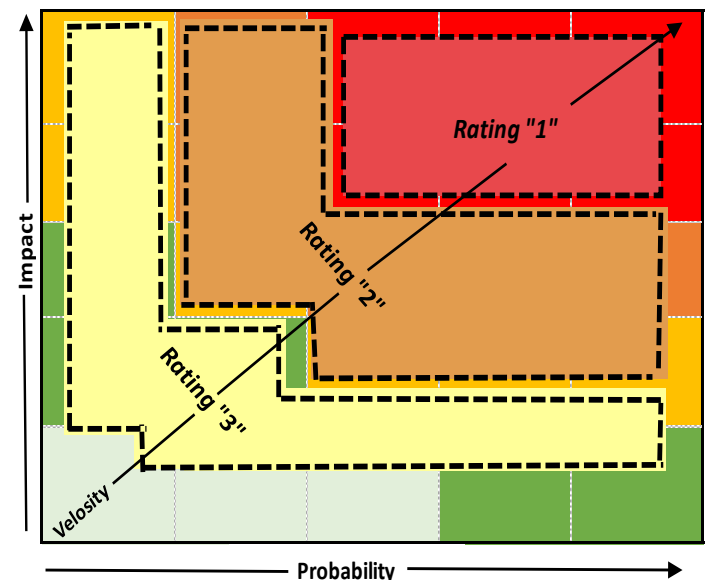
- More than remote probability for damage to the Company's reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls related are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

"3" Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

"4" – Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited



1) <u>Controls Over Adjustments to Northern Indiana Public Service Company (NIPSCO) Gas Emergency Response Exceptions</u>		Rating: 3
<u>Observation:</u> NiSource Inc. (NiSource or the Company) has established an emergency response time target of 45 minutes, and delayed emergency response is measured and monitored to ensure that associated process and training issues are identified and appropriately addressed. The delayed emergency response metric is tracked by Company leadership within the NiSource Balanced Scorecard, which provides quarterly updates on key performance measures and initiatives that cross the entire enterprise. Integration Center (IC) personnel review, validate and frequently adjust exceptions (almost 40% of exceptions are removed) to the emergency response time target prior to the delayed emergency response metric being calculated. Adjustments to NIPSCO Gas emergency response exceptions are not confirmed by a supervisor and documentation evidencing the reason for adjustments is not consistently retained. <u>Criteria:</u> Processes and controls related to monitoring emergency response time are adequate to ensure that monitored metrics are accurate and processes or training issues are identified and appropriately addressed; specifically: 1) response time exceptions are monitored timely; 2) exceptions adjustment processes are defined; 3) defined processes are consistently executed; 4) adjustments are reviewed and confirmed; and 5) adequate documentation to support processes is retained. <u>Risk:</u> Potential that delayed emergency response metrics are inaccurate leading to process and training issues not being identified and appropriately addressed. Also, potential that performance metrics and potentially compensation for some employees are impacted by incorrect metrics.	<u>Management Action Plan:</u> While the finding identified does not have a direct impact to emergency response processes executed in the field, IC management agrees with the audit finding and will update processes associated with the review and adjustment of NIPSCO Gas delayed emergency response to ensure appropriate review and adequate documentation for exceptions, including reason for the exception and supervisor approval. <u>Responsible:</u> Lloyd Tiffner, Director IC Field Operations <u>Resolution Date:</u> Processes are targeted to be redesigned and implemented by July 2022.	

2) <u>IC Application Access Controls</u>	<u>Rating:</u> 3
<u>Observation:</u> While users cannot access IC applications without authenticating to the Company's network using valid network credentials, controls to ensure the appropriateness of users' access to specific data or functions within the IC applications are not sufficient; specifically: 1) processes to grant, terminate or change application access permissions when users' roles and responsibilities change are not formalized and 2) access is not periodically reviewed and verified to ensure that access is consistent with the users' roles and responsibilities. We identified two users with inappropriate levels of access to the Delayed Priority Lotus Notes Database, an application which maintains information utilized to calculate the delayed emergency response metric. The incorrect access was corrected during the audit. <u>Criteria:</u> Controls are sufficient to ensure that access to data and application functions are appropriate and consistent with users' roles and responsibilities; specifically: 1) access to applications requires users to be authenticated to the Company's network using valid network credentials; 2) access requests are authorized by employees' direct supervisors and business data owners; 3) processes to terminate or change application access when users' roles and responsibilities change are formalized; and 4) access is periodically reviewed and validated to ensure granted access is appropriate in consideration of users' roles and responsibilities <u>Risk:</u> Potential that inappropriate user access to applications leads to data integrity, confidentiality and/or availability being compromised.	<u>Management Action Plan:</u> While there were minimal instances of improper access identified, IC management agrees with the audit finding and will update processes to ensure employees with access to applicable systems are periodically reviewed. The IC leadership team will review the current process to determine the appropriate steps required to satisfy the audit findings and will document the future processes. <u>Responsible:</u> Dan Williamson, Vice President Work Planning and Scheduling <u>Resolution Date:</u> Processes are targeted to be redesigned and implemented by October 2022.
3) <u>Close-Out Activities – System Processing Exceptions</u>	<u>Rating:</u> 4
<u>Observation:</u> To ensure activities performed in the field are timely and accurately reflected within the applicable work management and customer information systems, IC personnel are responsible for addressing daily	As it was determined that additional monitoring reports exist which would eventually identify unresolved exceptions, risk is limited and no management response was required; however, Internal Audit recommends that management consider whether establishing formal

generated system exceptions which identify when information entered by field technicians does not properly process within the intended system of record.

The system exception review processes are manual and subject to human error and controls to monitor the exception review processes are not formalized, which could result in exceptions being overlooked. While additional monitoring reports are generated and reviewed, these processes occur less frequently and delays in addressing system exceptions could have negative impacts on other key downstream processes (e.g., new business activities, mapping and recording, associated accounting and budgeting).

Criteria:

Controls are sufficient to ensure that system processing and interface exceptions are identified and addressed timely to ensure accurate and complete records of field activities and pipeline assets.

Risk:

System processing and interface exceptions may remain unresolved, preventing completed field activities from being reflected timely within systems of record and creating potential delays in other key downstream processes.

monitoring controls over the daily completion of system generated exceptions would enhance process consistency and efficiency.

***** End of Report*****

NiSource Corporate Services Company

NiSource Next Digital Field Enablement

Internal Audit Advisory Report

Distribution

Beneficiaries

Daniel Creekmur
Michael Rosello
Timothy Tokish

Carla Donev
Gregory Skinner
Marie Walker

Michael Hooper
Steven Sylvester
James Zucal

Other Key Personnel

Christopher Johnson

Kimberly Langfield
Don Tokoly
Linda Crowley

Akash Tiwari

For Information

Shawn Anderson
Donald Brown
Kim Cuccia
Charles Shafer
Violet Sistovaris
Pablo Vegas
Lloyd Yates

Internal Audit Advisory Report

Background

NiSource Inc. (NiSource or the Company) field employees utilize the Mobile Data Terminals (MDTs) to perform electric and gas related customer support functions. As mobile computer devices, MDT devices can communicate with the central dispatch office and provide employees access to information while they are in the field. The MDT devices were not part of the regular technology refresh cycle due to legal data preservation requirements, and the postponement of the NiSource Next Field Mobility Enterprise Schedule and Dispatch project into 2022 has further stretched the lifespan requirement of the devices. The aging devices are encountering widespread performance and connectivity issues. Therefore, the Information Technology (IT) team initiated an effort during 2021 to stabilize the devices by performing interim support and patching until problem devices can be permanently replaced. In addition to the stabilization efforts launched in 2021, the mobile device deployment project team is deploying tablet computers to field employees.

Most deployed mobile devices are Apple Inc. iPads (iPads), but in certain circumstances, the project team deploys Microsoft Corporation Surface Pro tablet computers. The primary objective of this initial mobile device deployment initiative is to improve connectivity and mobile mapping capabilities. Newly deployed iPads are not replacing MDT devices at this time. Field employees will continue to use their MDT devices alongside the new iPads. When Microsoft Surface Pro tablet computers are deployed, the tablets fully replace the MDT devices. Remaining MDT devices are expected to be replaced in 2023 after key field operations applications are modernized as part of the NiSource Next initiatives.

The newly deployed iPad devices are included in the pilot implementation of Microsoft Intune mobile management solution, a cloud-based technology management tool. The Intune solution has the capability to control the settings of various mobile devices and its operating systems; however, the pilot team has initially implemented and enabled the tool for deployed iPad settings only and the tool has not yet been enabled for all other mobile devices. Because the ongoing NiSource Microsoft Office 365 Enterprise project will fully utilize Intune capabilities, the Intune profile is expected to be fully implemented and tested as part of the enterprise-wide initiative.

Audit Objective, Approach, and Coverage

The objective of this advisory assessment was to evaluate the risk management practices designed to address the ongoing challenges with MDT devices and evaluate the effectiveness and efficiency of controls related to the mobile device deployment project. Key review areas of this assessment included: business risks related to MDT device challenges, ongoing IT MDT stabilization efforts and alignment to meet current business objectives, stakeholder communication efforts, inclusion of standards and controls to protect the integrity, confidentiality and availability of company data associated with continuing enterprise iPad deployments, and design and effectiveness of organizational change management (OCM) and device deployment processes in place to enable successful iPad usage by field employees.

During the advisory assessment, we specifically reviewed:

- Business risk management practices for the aging MDT devices
- Governance process and roles and responsibilities for the ongoing IT MDT stabilization initiative
- Stakeholder communication related to the MDT stabilization efforts
- Adherence to corporate IT security standards and policies associated with mobile device deployment project activities
- The establishment of NiSource's cyber, data security, and legal hold/retention requirements and how those are being tested, managed and approved for mobile device deployment project
- Design and effectiveness of organizational change management, training and mobile device deployment processes

- Effectiveness of iPad user acceptance and adoption activities and how those are meeting/not meeting current business objectives and customer-focused efforts

We did not evaluate MDT security settings. Additionally, we did not evaluate Microsoft Surface Pro security settings. These controls will be considered during future risk-based, integrated audit engagements.

Summary of Key Internal Audit Recommendations

The mobile device deployment team has successfully deployed over 2,400 mobile devices to date, which included developing job aids, administering training and providing hyper care support post device deployment. We conducted stakeholder and end user interviews during our review, and the information we obtained during these interviews indicates that the project team has some opportunities to enhance mobile device deployment communication processes and the training and post-deployment support experiences. We anonymized and shared detailed interview responses with the project team.

To address the MDT and mobile device connectivity issues in remote areas of NiSource's services territories, the mobile device deployment team piloted AT&T Inc. FirstNet communication platform dedicated to first responders and public safety agencies in the Columbia Gas of Maryland service territory. The team also deployed Verizon Communications Inc. Mobile Broadband Priority (MBP) service in several operating areas to address the data traffic challenges. While these pilot efforts were successful, the project team is analyzing the cost versus benefit of piloting available platforms in other remote areas of the Company's service territories. As device connectivity problems introduce operational challenges and inefficiencies, we recommend that the project team continue to explore opportunities to resolve connectivity issues in remote areas.

We observed some opportunities to further enhance the MDT Stabilization initiative efforts and Mobile Device Deployment project, and a summary of key recommendations follows:

1) Mobile Device Management Profile Configuration

The early Microsoft Intune device management profile proof-of-concept implementation was managed by a tiger team of IT specialists brought together to evaluate and adapt Microsoft's standard configuration settings to meet the Company's security requirements in advance of the Microsoft 365 enterprise rollout. The tiger team identified initial profile configuration settings to align with the NiSource IT Mobile Device policy and standard. However, rigorous documentation and technology change management processes were not followed, and the configuration settings established within the profile were not thoroughly validated prior to being deployed in production.

We evaluated the alignment of the Microsoft Intune profile configuration settings and documentation to the NiSource IT Mobile Device policy and standard, and we identified discrepancies in settings and documentation relative to the policy. Noncompliant security configuration increases the probability that mobile devices are not adequately secured, which could result in data integrity or confidentiality being compromised.

The project team is deploying a corrected profile and updating documentation found to be inconsistent with the NiSource IT Mobile Device policy and standard. We recommend that the IT team adhere to robust change management practices and formally validate profile configuration settings prior to implementing profiles into production.

2) MDT Stabilization Issues Management

The tiger team involved in the pilot implementation of Microsoft Intune profile also managed the ongoing MDT stabilization efforts. The team initially focused on identifying issues across the Columbia Gas of Kentucky footprint and then expanded these efforts to other NiSource service territories. The team has particularly focused on resolving challenges related to connectivity due to the age of the MDT devices and the older cellular modems in these devices.

While the tiger team has reported findings and results to executive leadership, the team has not established formal processes to track and manage identified issues through to resolution. Lack of governance over issues management and resolution increases the risk that identified issues are not fully addressed, which could result in rework and preventable problems not being avoided.

We recommend NiSource IT management align with gas operations leadership across NiSource service territories to jointly define the roles and responsibilities and issues resolution tracking processes, including key reporting activities. Embedding governance processes into the existing MDT stabilization efforts initiative will provide role clarity and cross-functional visibility into common MDT challenges while facilitating alignment of stakeholder support across the NiSource footprint.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. Internal Audit will perform an assurance review of mobile device security settings (including the Intune profile configuration settings) in future audits. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Advisory Report *****

Columbia Gas of Pennsylvania and Columbia Gas of Maryland

Operations General Controls Audit

Internal Audit Report

Distribution

Respondents

Curtis Anstead
Jennifer Douglas

Eric Belle
Adam Lanier

Raymond Brumley
Jennifer Sawyers

Beneficiaries

Brent Archer
Michael Hooper
William Mojica
Vincent Parisi

Kimra Cole
Paul Hunter
Dave Monte
David Roy
Daniel Williamson

Dan Douglas
Mark Kempic
Mahesh Nagarkatti
Steven Sylvester

Other Key Personnel

JR Barnhart
Michelle Rust

For Information

Shawn Anderson
Donald Brown
Kim Cuccia
Charles Shafer
Violet Sistovaris
Pablo Vegas
Lloyd Yates

Internal Audit Report

Background

Columbia Gas of Pennsylvania (CPA) and Columbia Gas of Maryland (CMD) are fully owned subsidiaries of NiSource Inc. (NiSource or the Company), and a single leadership team manages operations for both companies. CPA owns and operates over 7,500 miles of distribution mainline pipelines serving over 435,000 customers and CMD owns and operates 650 miles of distribution mainline pipelines serving over 35,000 customers. Ownership of service lines varies across the two companies. All service lines in CMD are owned by the Company, while approximately 30 percent of service lines in CPA are company-owned. The remaining 70 percent of service lines in CPA are customer-owned, meaning the customer is responsible for the installation and associated maintenance work on those assets while the company maintains certain oversight and compliance responsibilities. Additionally, CPA owns and operates the Blackhawk underground gas storage facility located in Beaver County, Pennsylvania.

CPA and CMD operations personnel are responsible for performing a wide range of operational activities to maintain and construct pipelines. The company utilizes a combination of third-party contractor resources and company employees, approximately half of which are union members subject to the requirements of collective bargaining agreements, to manage ongoing operations and complete new construction. Successful execution of operational activities requires clear planning processes and strong collaboration with various departments, including Engineering, Field Operations, System Operations, Construction and the Integration Center. The Gas Standards and Technical Training teams act as supporting functions and are responsible for establishing formal gas standards, policies, procedures and related training. The CPA and CMD operations team recently implemented enhanced construction planning activities to improve identification and mitigation of construction risk.

Audit Objective, Approach, and Coverage

The objective of this risk-based internal audit was to provide an independent evaluation of the effectiveness of general operations controls. At the beginning of our audit, we completed a risk assessment, and we conducted detailed process assessments, data analytics and sample-based transactional testing in higher-risk areas. The review period for this audit was January 2021 through October 2021.

During the audit, we specifically evaluated:

- Adherence to construction planning policies and procedures, with a particular focus on stakeholder reviews, tie-in plans, Gas Control Clearance Center communication and authorization and pre-construction activities
- Applicable operator qualification processes
- Timely completion of inspection and maintenance compliance activities, including those related to the operation of the CPA Blackhawk storage facility
- Compliance with specific requirements related to customer-owned service lines, including pressure testing and verification of plumber operator qualification
- Workforce management, with a focus on overtime monitoring, rest periods and other administrative requirements of union bargaining agreements

We did not evaluate third-party contractor monitoring activities as these activities will be reviewed during an audit planned to occur during 2022. Additionally, the scope of this review did not include equipment calibration requirements as CPA is currently addressing known process gaps associated with higher-risk equipment and revised processes are currently under development.

Internal Audit Finding Ratings

We assign ratings to audit findings based on the following scale (see the Internal Audit Finding Rating Scale in Appendix A):

“1” – Significant Improvement is Needed and Prompt Management Attention is Required

“2” – Improvement is Needed and Management Attention is Necessary

“3” – Some Improvement is Needed and Management Attention is Justified

“4” – Management Evaluation is Desirable

Internal Audit Conclusion and Summary of Observations

Senior leadership changes have been positive for the CPA and CMD team and are driving better collaboration and communication across the operations organization. Like other NiSource operations organizations, the CPA and CMD team are navigating a high volume of process, technology and organizational change, which could lead to unreliable and inconsistent execution. We recommend that management continue to assess the consolidated impact of changes and make the necessary adjustments to manage risks.

Overall, we found that processes and controls related to some of the areas tested (as specified in the “Audit Objective, Approach, and Coverage” section of this report) were generally operating as intended. We did, however, identify one finding associated with verification and documentation of operability for isolation valves included in the emergency shutdown plan section of tie-in plans that requires management’s prompt attention (Rating 1). We also identified four findings where management’s attention is necessary (Rating 2). In addition, we observed some less-significant items that were discussed with management during the audit.

A summary of audit findings rated “1” through “3” follows (see the Internal Audit Findings Matrix in Appendix B):

- 1) Isolation Valve Operability Assessment within Emergency Shutdown Plans (Rating 1)
The operability of isolation valves identified in the emergency shutdown plan section of tie-in plans is not consistently verified and recorded, increasing the risk of not being able to appropriately isolate the system in the event of an emergency.
- 2) Compliance Activities Related to Customer-Owned Service Lines (Rating 2)
Compliance activities related to customer-owned service lines that the Company is responsible for are not consistently executed or recorded, increasing the risk of public or employee safety events.
- 3) Non-Adherence to Gas Standard Requirements – Stakeholder Reviews (Rating 2)
Personnel are not adequately trained, and monitoring procedures are not sufficient to ensure that the Company’s records evidence that all required stakeholder reviews were properly performed and documented during various phases of the construction process, increasing the risk that potential risks or hazards associated with construction are unidentified and unmitigated.
- 4) Non-Adherence to Company Policy – Pre-Job Briefing (Rating 2)
Monitoring activities are not sufficient to ensure completion of pre-job briefing activities, which are required to ensure field personnel identify roles, responsibilities, risks and hazards before work begins.
- 5) Repetitive Task Creation and Monitoring (Rating 2)
Established policies and procedures and related monitoring processes are not sufficient to identify exceptions to required inspection and maintenance activities for pipeline assets, increasing the risk that compliance activities will be delayed or missed.

Management's Response

Management agrees with the findings noted during this audit and have provided action plans to address the risk identified. Detailed action plans are included in Appendix B. The key mitigation steps will be completed by December 31, 2022.

Internal Audit Follow Up

Management has provided action plans for all findings with a rating of "1", "2", or "3". We have reviewed management's action plans and believe that the action plans will adequately address the findings identified in this audit. We will track the progress of resolution and will conduct follow-up testing for all rated "1" audit findings and a sample of rated "2" and rated "3" audit findings.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Report *****

"1" Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company's reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

"2" Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

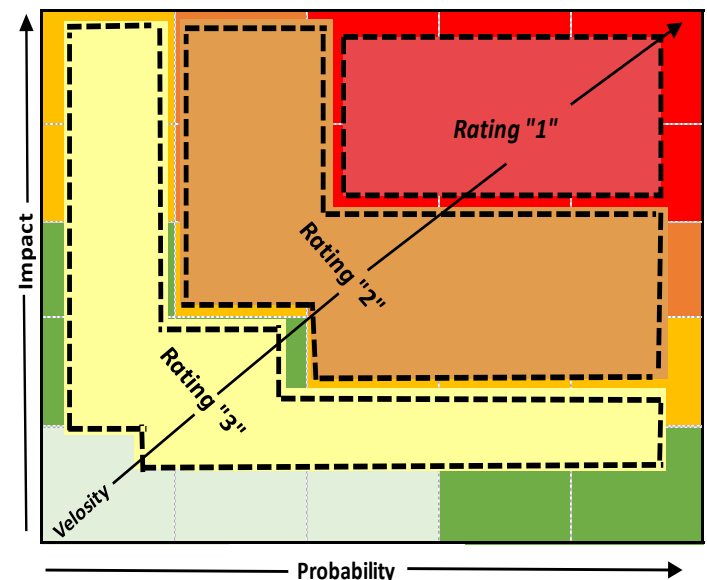
- More than remote probability for damage to the Company's reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls related are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

"3" Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

"4" – Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited



1) <u>Isolation Valve Operability Assessment within Emergency Shutdown Plans</u>	Rating: 1
<u>Observation:</u> The emergency shutdown plan section of the tie-in plan is designed by an engineer and confirmed by field personnel on the day of construction to enable a quick and effective response should emergency shutdown to protect life and property become necessary during the tie-in process. We assessed the emergency shutdown plan section of all tie-in plans executed from March 2021 to June 2021 and noted that processes should be improved to ensure emergency shutdown plans are feasible and records evidence that required validation procedures and risk assessment activities were performed on the day of construction. Current validation processes allow field personnel to confirm the operability of the isolation valves by referencing the results of the most recent annual inspection, which only occurs for valves designated as critical and could have occurred up to 15 months prior. Also, a process to confirm the operability of non-critical valves, which are not consistently inspected, is not defined. We found that 21 percent of the emergency shutdown plans reviewed included non-critical valves and five percent only included non-critical valves. We also found that 11 percent of the emergency shutdown plans would require turning more than five valves. As some crew members are not qualified to turn valves, this scenario may unacceptably increase the time that it takes to perform emergency shutdown procedures. <u>Criteria:</u> Processes and controls enable a quick and effective response to protect life and property should emergency shutdown become necessary during the tie-in process; specifically: 1) defined procedures are designed to consistently minimize public safety incident risk; 2) documented procedures and training enable execution consistency; 3) roles and responsibilities are clearly defined and understood; and 4) records retained accurately evidence field activities.	<u>Management Action Plan:</u> Columbia Gas of Pennsylvania (CPA) and Columbia Gas of Maryland (CMD) management have completed the following actions: • Clarified expectations for CPA and CMD engineers to populate the date and operable status of the last inspection for all critical valves included in the emergency shutdown plan section of the tie-in plan • Clarified expectations for CPA and CMD field personnel to physically validate operability of non-critical valves included in the emergency shutdown plan section of the tie-in plans Leadership for the remaining NiSource Gas Distribution Companies will complete the following actions: • Clarify expectations for engineers to populate the date and operable status of the last inspection for all critical valves included in the emergency shutdown plan section of the tie-in plan • Clarify expectations for field personnel to physically validate operability of non-critical valves included in the emergency shutdown plan section of the tie-in plans Additionally, NiSource gas management will assess and decide on the following items: • Appropriateness of including non-critical valves within the emergency shutdown plan section of the tie-in plan • The appropriate method to validate operability of isolation valves identified in the emergency shutdown plan section of the tie-in plan Once conclusions have been reached for the items above and consideration has been given to the impacts of any changes required,

<u>Risk:</u> Inoperable isolation valves increase the probability of negative outcomes resulting from an emergency event. Inaccurate and/or incomplete records increases legal risk.	NiSource management will establish processes to address the risk identified. <u>Responsible:</u> Curtis Anstead, Vice President Gas Operations Eric Belle, Vice President Engineering and Standards <u>Resolution Date:</u> Expectations for the implementation of remediation efforts are as follows: • CPA and CMD management clarified expectations for engineers and field personnel in January 2022 • Expectations for the remaining NiSource Gas Distribution Companies will be clarified by May 2022 • NiSource management will conclude on the decision points listed above by June 2022	
2) <u>Compliance Activities Related to Customer-Owned Service Lines</u>		<u>Rating:</u> 2
<u>Observation:</u> In certain service areas of CPA, customers own the service line assets and are responsible for engaging qualified plumbers to install, replace and repair their gas service lines in accordance with the requirements outlined in the CPA Plumber’s Guide. Subsequent to work being performed by a plumber on a customer-owned service line, a CPA technician is required to inspect and pressure test the service line before it is placed in service. Additionally, the CPA technician is required to create a paper service line record form, update related work management system data fields and verify that the plumber who performed the work on the customer-owned service line was properly qualified. Requirements related to customer-owned service lines are not always adhered to; specifically:	<u>Management Action Plan:</u> CPA management team will complete the following: • Communicate to field personnel the requirement to document verification of CPA plumber’s operator qualifications along with the plumber’s name and identification number in the additional information/remarks section of the service line record form until such time as the form can be revised to include a new field(s) to specifically document this information • Ensure quality assurance procedures performed over service line records include verification of pressure test readings recorded on the service line record and within the work management system and verification of CPA plumber operator qualifications • Ensure completion of existing open action plan related to establishing exception reporting and monitoring process related to	

- Evidence that a CPA technician verified the plumber's operator qualification as required was not consistently documented or retained
- Paper service line record forms are not consistently completed for customer-owned service line locations
- Pressure test readings are not consistently populated within the work management system, and we noted variances between the work management system and the associated paper service line record

Criteria:

Processes and controls are sufficient to ensure records evidencing execution of required tasks related to customer-owned service lines are created and retained; specifically, 1) roles and responsibilities are clearly defined; 2) impacted personnel are adequately trained and assessed for understanding of requirements; and 3) monitoring controls are sufficient to identify lack of adherence to requirements.

Risk:

Noncompliance with established processes results in increased potential of public or employee safety incidents. Also, potential for regulatory noncompliance if records are not appropriately captured and maintained.

service line record completeness for all Columbia Distribution Companies

Additionally, NiSource management has undertaken an initiative to implement digital service line records forms. These forms will be created and retained within the Mendex Forms application. As the Mendex application will require the completion of all fields before a form can be submitted and will allow for the collection of digital data which can be easily queried and analyzed, enhanced exception reporting and monitoring will be possible.

Responsible:

Curtis Anstead, Vice President Gas Operations
Jennifer Douglas, Director of Construction, System Operations, and Customer Programs
Jennifer Sawyers, Director Quality Management System Performance and Process Management

Resolution Date:

Expectations for the implementation of remediation efforts are as follows:

- Communication of expectations to document plumber operator qualifications on service line records will occur by May 2022
- Enhancement of quality assurance procedures will be completed by June 2022
- Full implementation and utilization of digital service line record forms and related exception and monitoring activities will be completed by December 2022

3) Non-Adherence to Gas Standard Requirements – Stakeholder Reviews

Rating: 2

Observation:

Gas standard 2810.050, “Stakeholder Reviews on Design Capital Projects”, has established requirements to complete and document review activities during various phases of the construction process to ensure potential issues which may create risk or impede construction are identified and addressed.

Personnel are not adequately trained, and monitoring procedures are not sufficient to ensure that the Company’s records evidence that required reviews were properly performed. We evaluated adherence to the stakeholder review requirements for a sample of job orders completed between March 1, 2021 and June 30, 2021 and noted inconsistencies related to the following:

- Thirty-three percent of the job orders reviewed did not include evidence that Pre-Construction reviews were completed by on-site personnel prior to the start of work
- One job order did not identify the project complexity (as determined by the responsible project engineer) within WMSDocs, a required step of the design review
- Formal approvals of tie-in plan advance briefing reviews (a process completed to ensure parties participating in construction indicate acknowledgment and agreement that the tie-in plan is accurate and addresses known risks) were not consistently retained

Criteria:

Capital project design processes are sufficient to appropriately manage risk related to capital construction activities; specifically: 1) procedures are designed to ensure thorough project risk evaluation by appropriate stakeholders; 2) personnel are appropriately trained and review processes are consistently executed; 3) activities are evidenced and records are retained such that the Company can demonstrate compliance with the established gas standards, policies

Management Action Plan:

NiSource Gas Operations & Construction management will complete the following:

- Develop monitoring procedures to ensure that Pre-Construction reviews are being performed and maintained within WMSDocs
- Reinforce expectations with field operations and construction personnel related to the completion and documentation of Pre-Construction reviews within WMSDocs and provide targeted training and communication

NiSource Gas Engineering management will complete the following:

- Reinforce expectations with project engineers regarding the requirements of maintaining documentation supporting the determination of project complexity within WMSDocs
- Clarify and communicate to project engineers the requirements of maintaining formal approvals of the tie-in plan advance briefing review process within WMSDocs

Responsible:

Curtis Anstead, Vice President Gas Operations
Raymond Brumley, Director Construction
Eric Belle, Vice President Engineering and Standards

Resolution Date

Clarification and communication of expectations for field operations, construction and engineering personnel will be completed by May 2022.
Monitoring procedures associated with Pre-Construction reviews will be established by October 2022.

and procedures; 4) monitoring activities are sufficient to identify noncompliance with standards, policies and procedures. <u>Risk:</u> Potential that risks associated with capital projects are not thoroughly considered and managed, which increases the probability of a public safety incident risk. Also, potential for regulatory noncompliance if records are not appropriately captured and maintained.	
4) <u>Non-Adherence to Company Policy - Pre-Job Briefing</u>	<u>Rating:</u> 2
<u>Observation:</u> CPA and CMD issued a new policy during 2021 which requires completion of a pre-job briefing for all field activities involving two or more personnel. The purpose of this policy is to identify roles, responsibilities, risks and hazards related to job order tasks before work begins. Additionally, the pre-job briefing process was updated in 2022 to include a daily acknowledgement step requiring the field personnel participating on the job to confirm their understanding of the job requirements and associated operator qualifications. Pre-job briefings are not consistently executed. Additionally, monitoring activities and feedback loops are not adequate to ensure the processes are effectively and consistently executed. Also, aspects of the policy are not sufficient to ensure that records evidencing completion of required activities are appropriately retained. We evaluated adherence to the policy requirements for a sample of job orders completed between March 1, 2021 and June 30, 2021 and noted: • Pre-job briefings were not retained for twenty percent of the job orders reviewed; although the pre-job briefing policy indicates that completed forms should be saved for three years, the policy does not specify the appropriate system of record and/or method of retention for completed forms, leading to inconsistent retention and missing forms • Fields and/or sections of the pre-job briefing forms are not consistently completed (sections are left blank), including the quality review section, which is a key step completed by the	<u>Management Action Plan:</u> NiSource management will complete the following short-term actions: • Begin utilizing digital pre-job briefing forms (created and retained within the Mendex Forms application) • Communicate a summary of the audit issues identified during the Quarterly Business Review and Cooperative Contractor Safety Committee meetings and reinforce pre-job briefing requirements, including the importance of recording the NiSource job order number on all completed forms • Utilize the contractor performance management team to conduct periodic reviews (integrated with contractor safety management system maturity assessments) of a sample of completed job orders to assess adherence to pre-job briefing requirements Additionally, NiSource management will undertake a long-term initiative to establish monitoring controls to ensure required pre-job briefings are completed for all job orders completed by company employees. <u>Responsible:</u> Curtis Anstead, Vice President Gas Operations Raymond Brumley, Director Construction Adam Lanier, Director Contractor Performance Management Jennifer Sawyers, Director Quality Management System Performance and Process Management

appropriate leader in the field to indicate that the construction plan was reviewed and approved - Two contractors were approved to utilize alternate versions of the pre-job briefing form; however, the alternate version of the forms completed did not include a reference to the CPA or CMD job order number, impairing the Company's ability to evidence that pre-job briefings were completed for all NiSource job order records - Quality assurance controls have not been established to provide feedback on the adequate completion and retention of the pre-job briefing process executed by third-party contractors <u>Criteria:</u> Process and controls are sufficient to ensure adoption of desired changes; specifically, 1) roles and responsibilities are clearly defined; 2) impacted personnel are adequately trained and assessed for understanding on new requirements; 3) monitoring controls are sufficient to identify lack of adherence to new requirements; and 4) impacts of changes are considered individually and cumulatively. <u>Risk:</u> Noncompliance with established policies and procedures results in increased potential of public or employee safety incidents.	<u>Resolution Date:</u> Short-term actions listed above will be completed by May 2022. Long-term actions will be complete by December 2022.
5) <u>Repetitive Task Creation and Execution</u>	<u>Rating: 2</u>
<u>Observation:</u> To manage compliance with inspection and maintenance requirements for various pipeline assets, repetitive tasks are utilized by all Columbia Distribution Companies, including CPA and CMD. Repetitive tasks are created within the work management system, which direct the system to automatically generate required job orders for the related pipeline assets in accordance with a designated frequency. Procedures are not sufficient to ensure repetitive tasks are consistently created with the appropriate frequency and validation controls are not in	<u>Management Action Plan:</u> NiSource management has corrected the eight repetitive tasks associated with critical valves that were found in error during the audit. Additionally, as the process issues apply to all Columbia Gas Distribution companies, the NiSource Gas leadership team will discuss the repetitive task process risks with the State Operations Consistency Council and the Risk Council to identify a leader to oversee risk reduction efforts across all Columbia companies.

place to ensure all facilities requiring compliance activities have established repetitive tasks. We assessed the population of repetitive tasks established as of August 2021 and noted that related job orders are being completed in accordance with designated frequencies; however, data parameters related to repetitive tasks are not always correctly established. We specifically identified that the designated frequency for eight repetitive tasks associated with critical valves was incorrectly established.

Additionally, a field within the work management system which indicates whether a repetitive task is required for the associated pipeline asset is not consistently and/or accurately populated. As a result, established exception reporting processes are impaired because exceptions are generated for non-required tasks. Also, exception reporting over repetitive tasks is not consistently worked and roles and responsibilities associated with this process are unclear. At the time of testing, there were approximately 800 assets identified as requiring compliance activities without a corresponding repetitive task established.

Criteria:

Processes and controls are sufficient to ensure compliance with required inspection and maintenance activities; specifically, 1) pipeline assets with an inspection or maintenance requirement are appropriately identified within the work management system; 2) repetitive tasks are appropriately created in accordance with established data parameters; 3) repetitive tasks are executed within required timelines; and 4) monitoring controls are sufficient to identify exceptions to established processes and lack of adherence to requirements.

Risk:

Potential for noncompliance with regulatory requirements.

After the identification of a process development action plan owner, a team will identify appropriate action items with target remediation dates to evaluate and redesign processes and controls related to the creation of facilities, establishment or repetitive tasks and associated monitoring and remediation activities.

Responsible:

Curtis Anstead, Vice President Gas Operations (designated as an interim responsible party to coordinate discussions with leadership councils)

Resolution Date:

Findings will be presented to leadership councils by May 2022. Remediation timelines for specific action plans will be determined at a later date.

6) <u>Non-Adherence to Rest Period Requirements</u>	<u>Rating: 4</u>
<u>Observation:</u> Upon working 16 or more hours within a 24-hour period, CPA and CMD union employees are required to a rest period specified in the applicable collective bargaining agreement; additionally, for safety reasons, all employees are sufficiently rested before performing work. We evaluated adherence to applicable rest period requirements and noted that, based on our analysis of pay periods from January 2019 through July 2021, response to emergency situations drove the eight exceptions identified. However, monitoring procedures and feedback loops could be enhanced to provide feedback to personnel and supervisors and emphasize safe operations and the importance of complying with rest period requirements. <u>Criteria:</u> Management monitors overtime hours and required rest period to ensure compliance with requirements of union collective bargaining agreements and maintain safe working conditions for all employees. <u>Risk:</u> Employees not receiving the appropriate amount of rest time can result in an increased safety risk (to the employee, public and facilities) due to the lack of alertness and focus that can result from fatigue.	As all exceptions to the required rest period identified were driven by emergency response work, risk is limited and no management response was required; however, Internal Audit recommends that management consider periodically performing an analysis of employee work hours to identify exceptions to union rest period requirements or company guidance and any outliers in overtime hours worked. Supervisors should be made aware of any exceptions and reminded of the importance of maintaining employee safety and wellness.
7) <u>Operator Qualification Management and Records</u>	<u>Rating: 4</u>
<u>Observation:</u> Controls to ensure that work is performed by properly qualified personnel are distributed and primarily rely on each individual to stop work when they are not qualified. While certain operator qualification verification controls have been established within the newly implemented construction planning processes, these controls are manual and can be bypassed.	A management response is not requested; however, Internal Audit recommends that management assess current processes and controls associated with operator qualification to ensure that proper qualification can be verified when a project is performed by more than one individual.

Project records do not indicate which operators complete particular tasks; as a result, the company does not have evidence that covered tasks were completed by appropriately qualified individuals. We identified instances where an employee had not completed the required daily acknowledgement (now combined with the pre-job briefing) but had charged time to a job order which included covered tasks where span of control would not apply, increasing the risk of non-compliance as the individual may be unaware of their qualifications.

Criteria:

Controls are sufficient to ensure that work is only performed by an individual who is properly qualified; specifically: 1) work tasks performed are clearly correlated with the necessary operator qualifications; 2) individuals formally validate proper qualification prior to performing tasks; 3) documentation exists to support adherence to operator qualification requirements; and 4) supervisors monitor that operator qualifications are kept current and timely address delinquencies.

Risk:

Potential for noncompliance with regulatory requirements resulting from lack of evidence that covered tasks were performed by appropriately qualified operators.

***** End of Report*****

NiSource Corporate Services Company

Critical Process Disaster Recovery and Business Continuity Advisory Review

Internal Audit Advisory Report

Distribution

Beneficiaries

Cecelia Largura
Ishreth Sameem

Other Key Personnel

Carla Donev
Margaret Rice

Stuart Grimes
Gregory Skinner

Kevin Johannsen
Timothy Tokish

For Information

Shawn Anderson
Donald Brown
Kim Cuccia
Charles Shafer
Violet Sistovaris
Pablo Vegas
Lloyd Yates

Internal Audit Advisory Report

Background

NiSource Corporate Services Company, a fully owned subsidiary of NiSource Inc. (NiSource or the Company) maintains two key functions with responsibilities pertaining to business continuity activities and disaster recovery capabilities for critical business processes. The Business Continuity team partners with functional areas across NiSource to facilitate the creation, testing, and ongoing management of approximately 260 business contingency and evacuation plans established to ensure the organization can respond to unforeseen events with the minimum possible disruption. As Information Technology (IT) is a critical component to the organization's operational processes, the IT organization also maintains a Disaster Recovery team responsible for establishing processes and plans to ensure IT assets, operations, applications, and infrastructure can resume normal operations after an unexpected event. NiSource's main data center is currently located in Hammond, Indiana. In the event of an incident, the approach for recovery is to utilize the secondary data center in Columbus, Ohio, if possible. Alternatively, the Company would use the SunGuard Availability Services facility near Philadelphia, Pennsylvania.

Audit Objective, Approach, and Coverage

The objective of this advisory assessment was to provide an independent evaluation on the effectiveness and efficiency of control structures related to restoration activities for critical technology infrastructure, along with how the enterprise maintains ongoing business operations if there is an unforeseen event. Key review areas of this assessment included: business continuity and disaster recovery alignment, disaster recovery continuous improvement activities and application disaster recovery testing.

During the advisory assessment, we specifically evaluated:

- Processes and controls established to facilitate information sharing between the Business Continuity and IT Disaster Recovery teams
- Continuous improvement activities, with specific focus on the enhancement of recovery runbook information and the completion of lessons learned activities resulting from disaster recovery exercises
- Application recovery plan processes and activities, including a detailed review of applications classified as high availability (Tier 1) and sample testing of rapid recovery (Tier 2) applications

We did not execute recovery exercises for any application, nor did we evaluate the scope or specific results of the prior recovery tests performed by the IT Disaster Recovery team. In addition, all controls and processes during this advisory review were evaluated as they existed at the time of the review, and not as part of the improvements which will be introduced during the upcoming disaster recovery modernization project.

Summary of Key Internal Audit Recommendations

While NiSource has formal processes in place related to technology recovery and business continuity, the Company recognizes opportunities to enhance existing processes and develop new capabilities to better enable the timeliness, reliability and efficiency of technology recovery activities and increased coordination between technology recovery and business continuity. The IT organization has initiated a disaster recovery modernization project with the goal of modernizing the recovery strategy, integrating the disaster recovery and business continuity programs, introducing periodic business impact analyses for all applications, and producing a more metric driven approach to drive continuous improvement.

During this advisory review, we observed some opportunities to further enhance current and developing activities and controls, and a summary of our key recommendations follows:

1) High Availability Application Testing:

Applications for which even limited downtime or data loss could result in significant negative impact to the NiSource business are labeled as “high availability”. Automatic failover recovery processes have been established for these applications, meaning the application runs concurrently in both the Hammond and Columbus data centers with one being deemed the primary and the other a secondary backup site. When the primary site has an issue or the application fails, the application automatically fails over to the backup site. This automatic failover should be tested routinely to ensure that the recovery process works and completes as intended.

Of 22 high availability applications in production, only 14 were formally tested as part of planned disaster recovery exercises. Six of the remaining applications were recovered because of scheduled maintenance or an event that forced failover, but two applications have not been tested since they were introduced into the production environment four years ago. Also, four high availability applications were incorrectly labeled in ServiceNow, the application portfolio management tool. These four applications were labeled as “active” within the production environment, but the actual status was “retired” or “pre-production”. Failure to periodically test all components of high availability application failover processes increases the risk that application failover is unsuccessful, which could result in outages or lost data. Additionally, incorrect labeling of the application status within ServiceNow increases the risk that appropriate disaster recovery support is not provided for an application.

We recommend a consistent testing schedule is established for all high availability applications to ensure the automatic failover solutions can be fully tested and validated for effectiveness. Further, we recommend that NiSource IT periodically review and validate the status within ServiceNow for all applications with disaster recovery requirements to ensure the production environment population is accurate and complete.

2) External Application’s Statement of Controls Documentation:

Several NiSource critical business functions utilize Software as a Service (SaaS) applications, meaning that while users access the application through the NiSource network, the application functionality is contained within the providers’ networks. While the NiSource IT organization does not maintain disaster recovery plans for these applications because disaster recovery efforts would be performed by the provider, NiSource should ensure that providers complete System and Organization Controls (SOC) assessments which attest to the effectiveness of their IT general controls, including disaster recovery controls. A current SOC document should be obtained and reviewed by NiSource annually to validate the effectiveness of the vendors’ control environments. NiSource IT did not request or maintain current SOC documents for the two SaaS applications sampled for testing. Failure to validate the sufficiency of technology controls, including disaster recovery controls, for key SaaS applications could result in NiSource not being aware of vendor control deficiencies that increase risks related to disclosure of sensitive information, data integrity and data/system availability, which impairs NiSource’s ability to appropriately manage these risks.

We recommend NiSource obtain and review SOC documents on an annual basis for all SaaS applications. As these SOC documents expire periodically and must be refreshed, we further recommend a department or team be assigned to manage this effort for the organization going forward and that processes are established to evaluate newly published SOC assessments and ensure the SaaS provider’s control environment is sufficient and controls are operating effectively. Additionally, management should consider whether user entity control responsibilities defined within SaaS providers’ SOC reports are effectively managed by NiSource.

3) Business Continuity and IT Disaster Recovery Team Alignment:

While the Business Continuity and IT Disaster Recovery teams share information on an informal basis, processes to ensure seamless coordination and consistent execution are not formalized. Also, roles and responsibilities and accountabilities for all key stakeholders (e.g., business application owners,

Legal and Corporate Communications) as it relates to business continuity and disaster recovery are not robustly and clearly defined. Failure to formalize processes and clearly define roles increases the risk of misalignment across stakeholder teams and execution gaps in business continuity and disaster recovery processes.

We recommend the Business Continuity and IT Disaster Recovery teams work together with other key stakeholders to create a RACI (Responsible, Accountable, Consulted, Informed) matrix for use during continuity and disaster related events. This structure should clarify roles and responsibilities during planning and testing activities in addition to incident response activities and should identify key roles and milestones such as who has the authority to declare an emergency in accordance with the associated risk of the incident, who is the overall coordinator for the event and when the event transitions from being an emergency to being handled in a steady state approach.

4) Business Impact Analysis:

Business Impact Analyses (BIAs) are used to determine proper disaster recovery coverage. To complete the analysis, both business and IT stakeholders must collaborate to determine what impact an outage would have for a particular application, including the impact of downtime and data loss. The best application recovery method can then be determined to meet the needs of the business. Although current processes require that a BIA is performed when new applications are introduced into the environment, these analyses are not periodically validated and refreshed. Failure to perform periodic application BIAs increases the risk that the established recovery method is misaligned with business needs, which could result in unacceptable application downtime or data loss because of an incident.

We recommend that the upcoming disaster recovery modernization project define criteria and timelines for performing periodic BIA reviews to evaluate if applications have the proper coverage needed to support NiSource business function and process needs.

5) IT Disaster Recovery Runbook Enhancements:

The IT disaster recovery runbook is a working document which outlines the necessary steps to recover from a disaster or service interruption and provides instructions for personnel responding to a disaster. A runbook should be kept up-to-date and current with the applications, technology, personnel, and other critical information needed to recover from a disaster or service interruption. The IT runbook currently utilized by NiSource IT is missing key information that would facilitate successful execution of a disaster recovery exercise. This missing information includes version control references, scope and objectives of the exercise, teams and contact information, roles and responsibilities of the teams and providers involved, tools and communication protocols, access and connectivity needs, problem reporting guidelines and templates and other information related to infrastructure or application recovery and validation testing. Insufficiently detailed runbooks may negatively impact the efficiency and effectiveness of personnel performing disaster recovery testing or responding to an incident.

We recommend NiSource IT develop a more comprehensive runbook containing, at a minimum, the components outlined above which can be used to support the testing and actual recovery of the IT environment in the case of an incident.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. Internal Audit will perform an assurance review of disaster recovery and business continuity processes in future audits. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Advisory Report *****

NiSource Corporate Services Company

Sensitive Customer Data Protection

Internal Audit Report

Distribution

Respondents

Michele Caddell

George Dice
Kevin Johannsen

Carla Donev

Beneficiaries

Jennifer Montague
Timothy Tokish

Other Key Personnel

Laura Chamberlain
James Keshian
Crista Reba

Venkatesh Iyer
Cecelia Largura
Laura Rosenthal

Kimberly Jones
Milind Mahale
Angela Sanchez

For Information

Shawn Anderson
Donald Brown
Kimberly Cuccia
Charles Shafer
Violet Sistovaris
Pablo Vegas
Lloyd Yates

Internal Audit Report

Background

NiSource Inc. (NiSource or the Company) serves approximately 3.7 million customers in six states. To conduct business and provide service to customers, NiSource must obtain and store customers' personal information (PI).

The NiSource Information Security and Privacy policies govern the classification and protection of the Company's data, including sensitive customer data. Highly sensitive customer data is considered PI and is classified as highly restricted or confidential. Policies specify how data should be protected by data classification. While policies provide data classification guidance, the Customer Service function is responsible for determining the classification of specific customer-related data elements. The information technology (IT) organization is responsible for implementing appropriate technology controls to ensure that data is protected in accordance with policy requirements.

Audit Objective, Approach, and Coverage

The objective of this risk-based audit was to provide an independent evaluation of the adequacy, effectiveness, and efficiency of processes and controls associated with sensitive customer data protection. At the beginning of our audit, we completed a risk assessment and reviewed policies, processes and controls in place at the time of our review.

We specifically evaluated:

- The adequacy of NiSource Policies and Standards, both Legal and IT, pertaining to information privacy, security and records retention
- Customer data protection and retention practices within NiSource's primary Customer applications, Customer Information System (CIS) and Distributive Information System (DIS), supporting cloud applications, and non-customer applications (i.e., corporate collaboration and storage repositories)
- Data encryption and transport settings for web portal systems and related interfaces containing sensitive customer data
- The effectiveness of vendor contracts, including the requirement for attestation reports from third party vendors who handle NiSource sensitive customer data
- The adequacy of sensitive customer data breach management plans and support activities

Internal Audit Finding Ratings

We assign ratings to audit findings based on the following scale (see the Internal Audit Finding Rating Scale in Appendix A):

"1" – Significant Improvement is Needed and Prompt Management Attention is Required

"2" – Improvement is Needed and Management Attention is Necessary

"3" – Some Improvement is Needed and Management Attention is Justified

"4" – Management Evaluation is Desirable

Internal Audit Conclusion and Summary of Observations

The Customer organization is dedicated to protecting sensitive customer information and has implemented robust procedures and practices to ensure that sensitive customer information is protected. The Company's policies

pertaining to information privacy, security and data retention are relevant and appropriately comprehensive. The policies are also assessed, updated and approved by proper personnel on a regular cadence.

While policies and operational procedures are generally sound, specific roles and responsibilities related to CIS and DIS data element classification and ongoing oversight of data protection and retention within the CIS and DIS platforms are not formally defined. Also, documentation demonstrating the alignment of data structures within these platforms to NiSource Legal policy requirements for sensitive data is not formalized. This lack of formality impairs the Company's ability to monitor and validate that CIS and DIS data security controls are operating as intended. We recommend that management: 1) formally define CIS and DIS data custodianship roles and responsibilities; 2) document data classification at the data element and screen level for data within the CIS and DIS platforms; and 3) periodically validate that user access to CIS and DIS sensitive customer data is appropriate.

Overall, we found that most processes and controls related to the areas tested (as specified in the "Audit Objective, Approach, and Coverage" section of this report) were generally operating as intended. We did, however, identify two findings where management's attention is necessary (Rating 2) and two findings where management's attention is justified (Rating 3). In addition, we observed some less-significant opportunities for improvement that were discussed with management during the audit.

A summary of audit findings rated "1" through "3" follows (see details in the Internal Audit Findings Matrix in Appendix B):

- 1) Protection of Sensitive Customer Data within DIS and CIS application platforms (Rating 2)
Data security controls related to the DIS and CIS platforms are not sufficient to ensure that all sensitive customer information is protected as required per policy. Specifically, three highly restricted customer data elements (Tax ID, Driver's License and Passport) stored within the CIS and DIS application platforms are not appropriately protected via limited security access or masking, and access to view some confidential customer data is granted to all CIS and DIS users with view-only access.
- 2) Verification of Third-Party Vendors' Controls for Cloud Applications (Rating 2)
Third-party vendors' controls related to cloud-based applications where sensitive customer data may be retained are not formally validated. Specifically, Systems & Organization Controls (SOC) 2 Type II reports are not periodically obtained and reviewed to ensure that vendors' controls relevant to protecting sensitive customer data are adequate and operating effectively.
- 3) Protection of Sensitive Customer Data Residing Outside of DIS and CIS (Rating 3)
While robust sensitive customer data management policies and procedures have been implemented by the Customer organization, technological controls have not been implemented for data residing outside of the DIS and CIS application platforms, and policies and manual processes may not be sufficient to ensure and verify consistent compliance with NiSource Legal policy.
- 4) Access to Sensitive Customer Data in Non-Production Application Environments (Rating 3)
While the IT Security policy prohibits copying sensitive customer data from production NiSource application environments to other NiSource application environments (e.g., development and test environments) without first taking appropriate security measures or obtaining appropriate approval, the ability to copy sensitive data from production is not technologically prevented, and violation of the policy may not be detected.

Management's Response

Management agrees with the findings noted during this audit and have provided action plans to address the risks identified. Detailed actions plans are included in Appendix B. The key mitigation steps will be completed by December 2022.

Internal Audit Follow Up

Management has provided action plans for all findings with a rating of "1", "2", or "3". We have reviewed management's action plan and believe that the action plan will adequately address the findings identified in this audit. We will track the progress of resolution and will conduct follow-up testing for all rated "1" audit findings and a sample of rated "2" and rated "3" audit findings.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Report *****

"1" Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company's reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

"2" Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

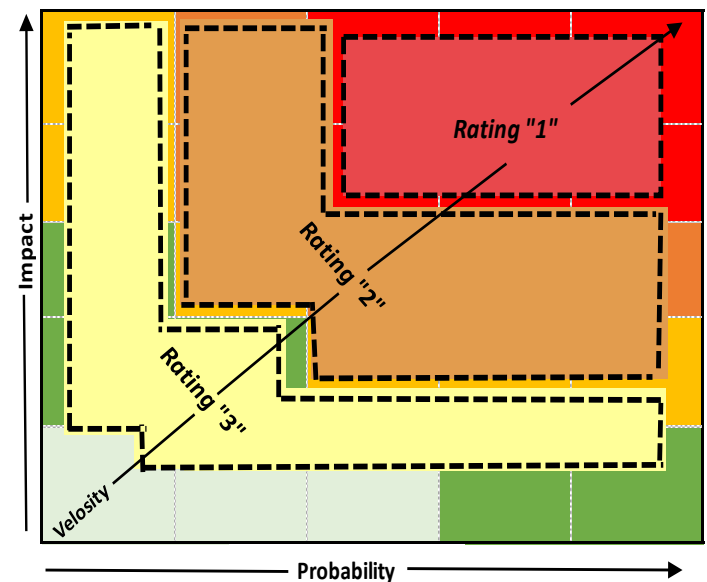
- More than remote probability for damage to the Company's reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls related are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

"3" Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

"4" – Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited



1) <u>Protection of Sensitive Customer Data within Distributive Information System (DIS) and Customer Information System (CIS) platforms</u>	<u>Risk Rating: 2</u>
<u>Observation:</u> Data security controls related to the DIS and CIS platforms are not sufficient to ensure that all sensitive customer information is protected as required per policy. Specifically, three highly restricted customer data elements (Tax ID, Driver's License and Passport) stored within the CIS and DIS platforms are not appropriately protected via limited security access or masking, and access to view some confidential customer data is granted to all CIS and DIS users with view-only access. <u>Criteria:</u> Controls are adequate to ensure that sensitive customer information within the primary NiSource Inc. (NiSource or the Company) customer information platforms is appropriately protected per policy; specifically: 1) the data structure for sensitive customer information is clearly understood and documented; 2) controls (access, masking, encryption, retention/removal) are appropriately applied; 3) controls are appropriately validated and monitored (particularly associated with significant support structure or application changes); and 4) data custodianship roles/responsibilities are clearly defined for involved parties. <u>Risk(s):</u> Potential that access to view sensitive customer information is not appropriately restricted leading to data being inappropriately disclosed and resulting in harm to the Company's reputation and potential legal risk.	<u>Management Action Plan:</u> The Customer Operations team will coordinate with the Information Technology (IT) Applications team on any future business processes that require the intake and storage of sensitive customer information to ensure that it is properly protected via limited security access and/or masking within the applicable customer information system. Additionally, the following actions will be completed to protect the sensitive customer data currently residing in the CIS and DIS systems: • Implement an annual review of DIS and CIS users who have "Read Only" access to ensure that access is appropriate • Implement quarterly access reviews for users with DIS Access Profiles (PI01-PI07) that allow unmasked viewing and updating of the restricted data elements (Note: Existing access reviews of CIS user profiles address the risk associated with viewing and updating sensitive customer data so no additional action is required for that application.) The IT Application team will also partner with the Customer Operations team to mask the Tax ID, Driver's License and Passport data elements within the production environments of the customer information systems, (CIS and DIS), to ensure users will not be able to view these full fields in the applications. <u>Responsible:</u> Michele Caddell (Customer Operations) Kevin Johannsen (IT Applications) <u>Resolution Date:</u> Remediation target dates for the action plans above are as follows: • Annual "read only" access reviews for CIS were completed in March 2022

	• Annual “read only” access reviews for DIS will be complete by April 2022 • Quarterly access reviews for DIS users with access profiles PI01-PI07 will be complete by April 2022 • The masking solution will be implemented by October 2022
2) <u>Verification of Third-Party Vendors’ Controls for Cloud Applications</u>	<u>Risk Rating: 3</u>
<u>Observation:</u> Third-party vendors’ controls related to cloud-based applications where sensitive customer data may be retained are not formally validated. Specifically, Systems & Organization Controls (SOC) 2 Type II reports are not periodically obtained and reviewed to ensure that vendors’ controls are adequate and operating effectively. In addition, normally expected complimentary user controls (which are controls that should be implemented by NiSource), such as periodic user access reviews, are not formalized and validated. <u>Criteria:</u> Controls are adequate to ensure the following: 1) sensitive customer data being retained by third party vendors outside of the NiSource network is being properly maintained, with access to view, modify or delete that sensitive customer data being appropriately restricted, 2) complimentary user control considerations within each third-party vendor attestation control report are being performed by NiSource. <u>Risk(s):</u> Potential that sensitive customer data retained by third party vendors on cloud platforms is not properly maintained by the third party vendor and/or complimentary user controls are inadequate, which increases the risk of inappropriate access to or disclosure of sensitive customer data.	<u>Management Action Plan:</u> To ensure appropriate access to sensitive customer data in third party systems, the Customer Operations team has established the following processes to perform access reviews for the Equifax, Intrado West, and Paymentus applications: • Implement semi-annual access reviews (occurring in the first and third quarter of the calendar year) for the Equifax and Intrado West applications • Implement semi-annual access reviews (occurring in the second and fourth quarter of the calendar year) for the Paymentus application As an initial step to assess risk related to our third party IT vendors, a program was established near the end of 2021 to conduct detailed Vendor Control Assessments (200+ question questionnaires) and address key findings as appropriate. Additionally, for the three vendors receiving sensitive customer data (Equifax, Intrado West, and Paymentus), the IT Risk organization will annually solicit SOC2 Type II reports and will evaluate and take action if necessary. <u>Responsible:</u> Michele Caddell (Customer Operations) Carla Donev (IT Governance Risk Management)

	<u>Resolution Date:</u> Remediation target dates for the action plans above are as follows: • Third Party Access reviews for Equifax and Intrado West were completed in February 2022 • Paymentus Access review will be complete by June 2022 • Assessment of SOC2 Type II reports for Equifax, Intrado West and Paymentus (including identification of any additional remediation required) will be complete by June 2022
3) <u>Protection of Sensitive Customer Data Residing Outside of DIS and CIS</u>	<u>Risk Rating: 3</u>
<u>Observation:</u> While robust sensitive customer data management policies and procedures have been implemented by the Customer organization, technological controls have not been implemented for data residing outside of the DIS and CIS application platforms, and policies and manual processes may not be sufficient to ensure and validate consistent compliance with NiSource Legal policy. Specifically, an enterprise Data Loss Prevention (DLP) platform is not implemented. Also, the tool (Cloud Access Security Broker) used to monitor for and block, per established configurations, certain data from being stored in cloud-based applications (specifically, BOX, Microsoft Office 365 and ServiceNow) is not configured to ensure compliance with all NiSource Legal policy requirements regarding sensitive customer information. <u>Criteria:</u> Controls are adequate to ensure sensitive customer data resident outside of the CIS and DIS application platforms is identifiable and protected as required per NiSource Legal policy. <u>Risk(s):</u> Potential that sensitive customer information inappropriately disclosed and results in harm to the Company's reputation and potential legal risk.	<u>Management Action Plan:</u> While IT management has evaluated a dedicated enterprise DLP solution and has determined based on the cost, scope and implementation timelines that this solution will be part of the future-state roadmap for NiSource IT, IT management commits to assessing existing toolsets that contain Data Loss Prevention (DLP) capabilities, such as ProofPoint, Palo Alto, O365 and CrowdStrike, to determine if additional capabilities can be configured to further monitor and alert/block sensitive customer data. <u>Responsible:</u> Carla Donev <u>Resolution Date:</u> Assessment of existing toolsets will occur by December 2022

4) <u>Access to Sensitive Customer Data in Non-Production Application Environments</u>	<u>Risk Rating: 3</u>
<u>Observation:</u> While the IT Security policy prohibits copying sensitive customer data from production NiSource application environments to other NiSource application environments (e.g., development and test environments) without first without taking appropriate security measures or obtaining appropriate approval, the ability to copy sensitive data from production is not technologically prevented, and violation of the policy may not be detected. <u>Criteria:</u> Sensitive customer data is prevented from being copied out of production NiSource application environments and leveraged in lower-level NiSource application environments without first being masked, redacted, purged or signed off by the CISO (or delegate). <u>Risk(s):</u> Potential that access to view sensitive customer information is not appropriately restricted leading to data being inappropriately disclosed and resulting in harm to the Company's reputation and potential legal risk.	<u>Management Action Plan:</u> Customer Operations will complete the following to help protect sensitive data in non-production CIS/DIS environments: - Implement an annual review of DIS and CIS non-production users to ensure that access is appropriate The IT Applications team will partner with the Customer Operations team to implement a solution that will scramble the defined data from the customer billing production environments as it migrates down into the non-production environments. <u>Responsible:</u> Kevin Johannsen (IT Applications) Michele Caddell (Customer Operations) <u>Resolution Date:</u> Remediation target dates for the action plans above are as follows: - Annual access reviews for non-production CIS and DIS users will be complete by July 2022 - The solution to scramble the defined data within the non-production environments of DIS and CIS will be implemented by December 2022
5) <u>Integration of IT Data Encryption and Transport Requirements into IT Project Delivery</u>	<u>Risk Rating: 4</u>
<u>Observation:</u> Data encryption and transport control requirements are not currently embedded within NiSource's IT Project Management Office (PMO) solution delivery checklists. <u>Criteria:</u> Data encryption and transport control requirements, which support sensitive customer data protection, have been integrated into	A management action plan is not requested; however, Internal Audit recommends that IT management align to enhance the Company's primary IT solution delivery methodologies (waterfall and agile) to include data encryption and transport standards as requirements. The data encryption and transport standards should then be made traceable at a detailed requirement level for any necessary testing to be executed prior to either solution go-live (waterfall) or minimum viable product release (agile).

NiSource's various IT project delivery methodologies to support testing traceability and compliance adherence.

Risk(s):

Potential that controls to ensure that sensitive data is properly encrypted and transported using secure protocols are inconsistently applied.

***** End of Report*****

NiSource Corporate Services Company

Capital Accounting

Internal Audit Report

Distribution

Beneficiaries

Gunnar Gode

Kevin Johannsen

Timothy Tokish

Other Key Personnel

Diego Castillo

Christopher Cubenas

Kristen King

For Information

Shawn Anderson

Donald Brown

Kimberly Cuccia

Charles Shafer

Violet Sistovaris

Pablo Vegas

Lloyd Yates

Internal Audit Report

Background

NiSource Inc. (NiSource or the Company), as part of the NiSource Next transformation, implemented capitalization policy changes to better enable: 1) consistency, 2) prudent operational and maintenance (O&M) cost management, 3) improved record accuracy and 4) proper asset capitalization. The new policy requires the capitalization of job orders to replace pipe or conductor wire of one foot or greater (one-foot rule). These changes became effective for Northern Indiana Public Service Company (NIPSCO) on July 3, 2021, and for the Columbia Distribution Companies (CDC) on September 20, 2021.

As part of the NiSource Next Evolution of Business Services initiative to drive efficiency and reduce costs, selected transactional activities (such as reconciliations, journal entries and report creation) previously performed by CDC and NIPSCO Fixed Asset Accounting teams were outsourced to Tata Consultancy Services (TCS). As a result of the outsourcing, the NiSource Fixed Asset Accounting team has been reduced from fifteen to eight employees, with the remaining team members responsible for performing analytical and strategic capital accounting activities and overseeing activities performed by TCS. The fixed asset subledger is maintained in the PowerPlant Asset Accounting (PowerPlant) software. Separate work management systems are used by the CDC subsidiaries and NIPSCO, and certain data elements are transferred between PowerPlant and the work management systems.

Audit Objective, Approach, and Coverage

The objective of this risk-based internal audit was to provide an independent evaluation of the effectiveness and efficiency of processes and controls related to capital asset records and accounting activities. At the beginning of our audit, we completed a risk assessment, and we conducted detailed process assessments, data analytics and sample-based transactional testing in higher-risk areas. The review period for this audit was January 2021 through February 2022.

During the audit, we specifically evaluated:

- Adherence to capital policies and procedures, with a particular focus on implementation of the one-foot rule
- Controls and monitoring to ensure the effectiveness of outsourced activities
- Controls to ensure the appropriateness of depreciation rates in PowerPlant
- Controls to ensure capital assets are timely and accurately recorded, with a particular focus on the accuracy of in-service dates
- PowerPlant application user access controls

We did not evaluate processes and controls related to technology asset accounting or asset retirement obligations. These processes will be evaluated in future audits. Due to limited visibility to capital changes in the NIPSCO work management application, we also did not test capital changes initiated by NIPSCO field personnel associated with the one-foot rule.

Internal Audit Finding Ratings

We assign ratings to audit findings based on the following scale (see the Internal Audit Finding Rating Scale in Appendix A):

“1” – Significant Improvement is Needed and Prompt Management Attention is Required

“2” – Improvement is Needed and Management Attention is Necessary

“3” – Some Improvement is Needed and Management Attention is Justified

“4” – Management Evaluation is Desirable

Internal Audit Conclusion and Summary of Observations

Capitalization policy changes have been successfully implemented and are expected to drive over \$11 million in O&M savings for 2022. Associated with the NiSource Next Evolution of Business Services initiative, the CDC and NIPSCO Fixed Asset Accounting teams were consolidated into a single NiSource team, and the consolidated team is operating as designed and effectively. Monthly and quarterly accounting close activities performed by TCS are being completed in accordance with key performance indicators with the appropriate review and oversight by the NiSource Fixed Asset Accounting team.

We did, however, note that decision points and activities related to adhering to the newly implemented one-foot rule are distributed and involve manual intervention by field personnel, which increases the potential of process inconsistency and policy non-compliance. Additionally, the capital work order flag is not a required field within the CDC work management system, which may result in further inconsistencies in process execution and the completion of work order records which do not definitively indicate whether the one-foot rule applied. We recommend management consider adjusting system configurations, including possible incorporation to the enhancements currently underway to implement a capital work order flag in the NIPSCO work management application, to make the capital work order flag a required field to ensure proper and consistent attention from field personnel. We also recommend enhancing and formalizing monitoring controls to ensure that transactions incorrectly capitalized using the capital work order flag are timely identified, addressed and personnel are retrained when appropriate.

Overall, process and controls related to the areas tested (as specified in the Audit Objective, Approach, and Coverage” section of this report) were generally operating as intended, and we did not identify any notable findings. We did, however, include one less-significant opportunity for improvement (Rating 4) in Appendix B and discussed some other opportunities for improvement with management during the audit.

Management’s Response

As we did not identify any notable findings (levels 1-3), a management response was not requested.

Internal Audit Follow Up

Management action plans were not requested as we did not report any notable findings. We will evaluate the adequacy, effectiveness, and efficiency of newly implemented controls during the next internal audit of Capital Accounting processes.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Report *****

"1" Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company's reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

"2" Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

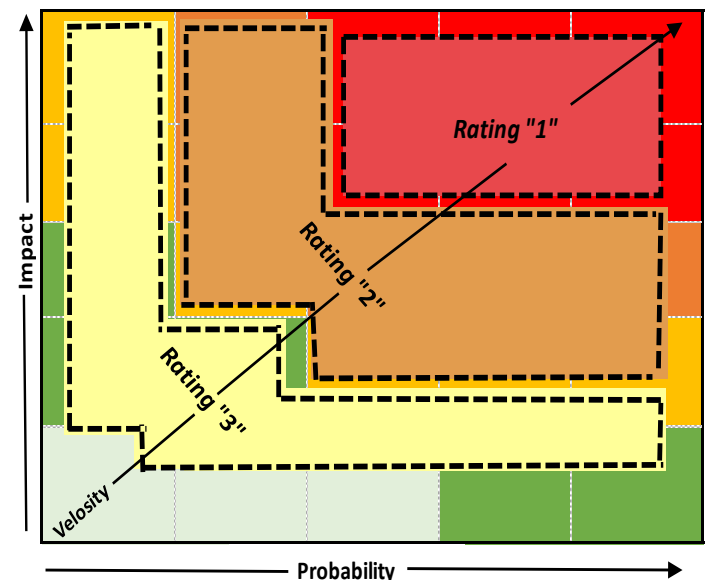
- More than remote probability for damage to the Company's reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls related are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

"3" Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

"4" – Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited



1) <u>Sarbanes-Oxley (SOX) PowerPlant User Access Control Testing Documentation</u>	<u>Rating:</u> 4
<u>Observation:</u> While the Sarbanes-Oxley (SOX) control established to validate appropriate user access to the PowerPlant Asset Accounting (PowerPlant) software was properly tested by the Information Technology (IT) SOX team during the third quarter of 2021, the SOX team member and process owner did not sign off on the control in the SOX data management application. As a result, it appeared that control testing was not properly executed and reviewed by the process owner. <u>Criteria:</u> Processes and controls are appropriate to ensure that SOX controls are properly executed and tested; specifically: 1) controls are timely executed and evidenced; 2) controls are tested; and 3) testing is properly documented, including formal sign-off by the process owner and the SOX team member in the SOX data management application. <u>Risk:</u> Potential for inappropriate access to PowerPlant and data if testing was inappropriate and not reviewed by the process owner.	A management response is not requested. However, Internal Audit recommends that Capital Accounting and the SOX team monitor completion of assigned SOX control testing to ensure that controls are timely tested and testing completion is properly evidenced.

***** End of Report*****

Columbia Gas Companies

Distributive Information System Customer Billing General Controls

Internal Audit Report

Distribution

Respondents

Kimberly Jones

Kristen King
Kenneth Smith

Angela Sanchez

Beneficiaries

Michele Caddell
Gunnar Gode

Carla Donev
Jennifer Montague
Timothy Tokish

Dan Douglas
Paula Strauss

Other Key Personnel

Laura Rosenthal
Derek Ziolkowski

For Information

Shawn Anderson
Donald Brown
Kimberly Cuccia
Charles Shafer
Violet Sistovaris
Pablo Vegas
Lloyd Yates

Internal Audit Report

Background

NiSource Inc. (NiSource or the Company) owns five distribution subsidiaries under the Columbia Gas brand (Columbia Gas Companies) that provide natural gas to approximately 2.4 million residential, commercial and industrial customers in Ohio, Pennsylvania, Virginia, Kentucky, and Maryland. Bills for all residential customers and most small commercial customers for the Columbia Gas Companies are generated utilizing recorded consumption and billing rates programmed within the Distribution Information System (DIS). Billing rates are calculated according to commission-approved tariffs.

Billing exceptions are generated based on programming established in DIS to identify outliers in consumption and indicate when certain administrative actions are necessary on a customer account. Certain exceptions are classified as actionable, meaning action is required before the bill can be sent to the customer. During our audit period, approximately 460,000 actionable exceptions were generated on customer accounts. Prior to October 8, 2021, all billing exceptions were reviewed and addressed by NiSource employees; however, as of October 8, 2021, the billing exception processes are largely outsourced to Tata Consultancy Services (TCS), a third-party service provider. A small number of NiSource employees are responsible for executing governance and quality assurance related to outsourced activities.

Audit Objective, Approach, and Coverage

The objective of this risk-based internal audit was to provide an independent evaluation of the adequacy, effectiveness, and efficiency of controls associated with the customer billing process executed within DIS for the Columbia Gas Companies. At the beginning of our audit, we completed a risk assessment, and we conducted detailed process assessments and sample-based transactional testing in higher-risk areas. The review period for this audit was November 2020 through October 2021.

During the audit, we specifically evaluated:

- Accuracy and completeness of billing components, including completeness of volumetric meter reads (and the associated system interface controls), rate creation and rate entry
- Controls over DIS access granted to create or update billing rates
- Billing exceptions processes and controls, including quality assurance activities and third-party performance monitoring

We did not evaluate billing processes occurring outside DIS as those processes are being evaluated in a separate audit. Additionally, we did not evaluate new business processes (e.g., new customer set up) and bill printing and mailing, as these processes will be considered for future reviews.

Internal Audit Finding Ratings

We assign ratings to audit findings based on the following scale (see the Internal Audit Finding Rating Scale in Appendix A):

“1” – Significant Improvement is Needed and Prompt Management Attention is Required

“2” – Improvement is Needed and Management Attention is Necessary

“3” – Some Improvement is Needed and Management Attention is Justified

“4” – Management Evaluation is Desirable

Internal Audit Conclusion and Summary of Observations

NiSource employees within the Billing Exceptions team that oversee TCS performance have extensive experience and insight into the customer billing processes and consistently and effectively interface with TCS to address identified issues. Recently, the team added additional resources who are performing independent quality assurance reviews over activities performed by TCS, which we believe will enhance NiSource's ability to monitor TCS performance, timely address issues and drive execution improvement.

While the level of procedural documentation is expansive and time spent on knowledge transfer from NiSource employees to TCS has been significant, procedural deviations continue to occur and some processes are not efficiently executed by TCS, particularly related to billing exceptions and adjustments. After our audit period, TCS completed an adjustment on a single customer account which resulted in an overbilling and overstatement of revenue for \$1.2 million for the month of December 2021. The Billing Exceptions team has established additional processes and controls for TCS to execute which would facilitate identification of material improper adjustments. We recommend that the NiSource Billing Exception team continue to work with TCS to improve process execution and monitor for proper adoption of these new adjustment review processes.

Overall, we found that processes and controls related to the customer billing process (as specified in the "Audit Objective, Approach, and Coverage" section of this report) were generally operating as intended. We did, however, identify three findings where management's attention is justified (Rating 3). In addition, we observed some less-significant items that were discussed with management during the audit.

A summary of audit findings rated "1" through "3" follows (see the Internal Audit Findings Matrix in Appendix B):

- 1) Third Party Quality Assurance Processes (Rating 3)
Quality assurance procedures performed by TCS over customer billing processes do not align with requirements outlined in the agreement between TCS and NiSource, increasing the risk that billing exceptions are improperly closed and/or billing adjustments are inappropriate.
- 2) Robotic Process Automation (RPA) Implementation (Rating 3)
User acceptance testing and post implementation validation controls were not sufficient to identify RPA programming errors, increasing the risk of delayed or inaccurate customer billing.
- 3) Customer Billing SOX Control Process Validation (Rating 3)
Sarbanes Oxley (SOX) control design assessment activities are not sufficient to consistently identify gaps in risk management or reflect changes to process execution.

Management's Response

Management agrees with the findings noted during this audit and indicated that action plans to address the risk identified have been completed. Detailed action plans are included in Appendix B.

Internal Audit Follow Up

Management has provided action plans for all findings with a rating of "1", "2", or "3". We have reviewed management's action plans and believe that the action plans will adequately address the findings identified in this audit. We will track the progress of resolution and will conduct follow-up testing for all rated "1" audit findings and a sample of rated "2" and rated "3" audit findings.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Report *****

"1" Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company's reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

"2" Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

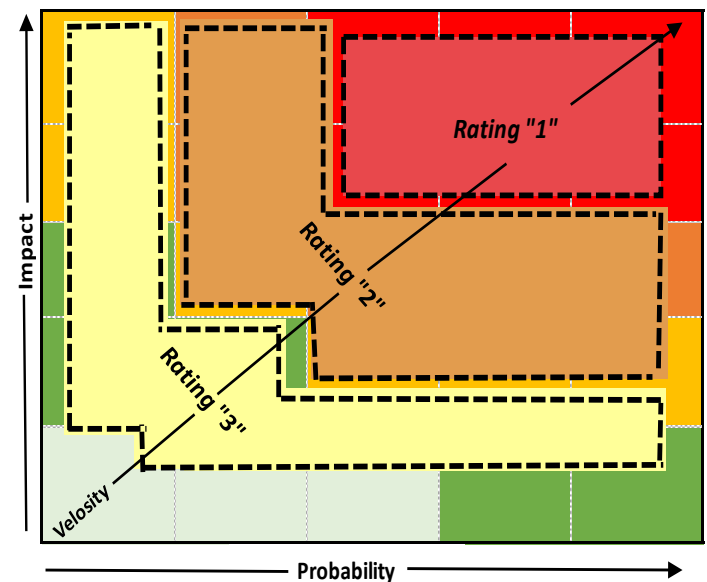
- More than remote probability for damage to the Company's reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls related are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

"3" Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

"4" – Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited



1) <u>Third Party Quality Assurance Processes</u>	<u>Rating:</u> 3
<u>Observation:</u> As part of the agreement between NiSource and Tata Consulting Services (TCS), TCS is required to perform quality assurance activities over closed billing exceptions, which facilitates identification of error trends and appropriate follow-up action to ensure billing exceptions are addressed according to NiSource policies and procedures. The agreement between TCS and NiSource requires that quality assurance reviews are conducted over billing adjustments; however, the TCS quality assurance processes do not cover the full population of billing adjustments and do not obtain appropriate coverage of higher-risk adjustments impacting customer balances. Additionally, TCS personnel performing quality assurance reviews over billing exceptions and adjustments did not always reach the appropriate conclusions. Also, required feedback and coaching sessions are not consistently and effectively performed or evidenced. <u>Criteria:</u> Quality assurance processes are adequately documented and executed to ensure billing exception process execution deficiencies are identified and corrected, specifically: 1) roles and responsibilities of those performing quality assurance activities are clearly defined; 2) the scope of quality assurance procedures is clearly defined and sample sizes are sufficient and appropriately focused; 3) quality assurance testing aligns with requirements documented within the agreement between NiSource and the third-party service provider; 4) results of quality assurance activities are recorded and properly communicated; 4) relevant feedback and coaching is provided; 5) corrective actions are taken or process adjustments are made for any issues identified; and 6) NiSource governance activities are sufficient to assess the adequacy and appropriateness of the review. <u>Risk:</u> Potential that billing exception process deficiencies are not identified and addressed leading to ineffective processes that delay or impact the	<u>Management Action Plan:</u> The NiSource Billing Exceptions team has completed the following actions in response to the audit observations: • Supplemented the Billing Exceptions team with additional resources to increase oversight and governance of TCS activities, particularly related to oversight of the quality assurance review processes executed by TCS • Implemented bi-weekly meetings with TCS to provide feedback on critical items identified by NiSource, including execution errors and trends identified as a result of the Error and Questions tracker maintained by NiSource Billing Exceptions and Payments • Began requesting and reviewing support for required feedback activities and following up on noted issues • Aligned with TCS on how adjustment processes should be incorporated into established quality assurance reviews with specific focus on performing daily reviews of any adjustment transactions over 100 cubic feet <u>Responsible:</u> Angela Sanchez (NiSource Billing Exceptions) <u>Resolution Date:</u> Complete as of March 2022

accuracy of customer bills. Also, potential that inefficiencies are not addressed, which could negatively impact costs.	
2) <u>Robotic Process Automation Implementation</u>	<u>Rating:</u> 3
<u>Observation:</u> NiSource utilizes multiple Robotic Process Automations (RPAs) programmed within the customer billing system to systematically close certain billing exceptions. We reviewed a sample of billing exceptions systematically closed during the period of November 2020 through October 2021 and identified that an RPA implemented in January 2021 was not functioning as intended, which resulted in six billing exceptions being inappropriately closed during the review period. While user acceptance testing was performed, the design of the testing did not identify programing errors. Additionally, a manual validation step to review all exceptions closed by the RPA was not effectively performed and did not identify the inappropriately closed memos. Although the improper function of the RPA remained undetected, the inappropriately closed exceptions did not ultimately manifest in billing errors. <u>Criteria:</u> RPAs are tested and validated for effectiveness, specifically: 1) user acceptance processes are sufficiently designed and executed and corrective actions are taken, if necessary, prior to implementation; 2) post implementation validation controls are sufficiently designed and executed. <u>Risk:</u> RPAs are not adequately tested and validated for effectiveness, potentially resulting in delayed or inaccurate customer billing.	<u>Management Action Plan:</u> The IT team responsible for RPA development and implementation corrected the programming error identified during the audit to ensure proper functionality in the future. Additionally, the IT management team will enhance RPA development standards and procedures to ensure user acceptance testing is properly designed, including gaining alignment with business process owners on the expected acceptance criteria and running test scenarios that sufficiently emulate production data. The NiSource Billing Exceptions team will validate exceptions systematically closed by RPAs daily to ensure issues with RPA functionality are timely identified and communicated to IT. <u>Responsible:</u> Kenneth Smith (IT) Angela Sanchez (NiSource Billing Exceptions) <u>Resolution Date:</u> Complete as of March 2022
3) <u>Customer Billing SOX Control Process Validation</u>	<u>Rating:</u> 3
<u>Observation:</u> Controls within the customer billing processes which have been identified as key to accurate, complete and reliable financial reporting are designated by the Accounting department to comply with Section	<u>Management Action Plan:</u> The SOX team has undertaken an initiative to improve control design assessment processes, enhance control process documentation, and confirm control description wording for key controls. Walkthroughs over

404 of the Sarbanes Oxley (SOX) Act. Process owners are responsible for the execution and testing of the controls and are required to notify Accounting when changes to the associated processes occur to ensure control descriptions are updated. SOX control design assessment activities are not sufficient to consistently identify gaps in risk management or reflect changes to process execution. We reviewed the designated SOX controls associated with customer billing processes and noted that some control descriptions should be updated; specifically:

- A designated SOX control to verify the customer billing system receives complete meter reading data is not performed within a billing cycle, creating the risk of delays in customer billing; however, a separate SOX control performed by the Information Technology department is performed daily which fully addresses the identified risk. Performing both controls is redundant and inefficient
- The description of a designated SOX control designed to ensure management identifies concerning trends in customer billing exceptions references reporting activities that do not occur because the associated processes have been outsourced to TCS

Criteria:

Customer billing SOX controls are sufficient to mitigate financial reporting risk; specifically: 1) control descriptions reflect current processes; 2) controls are appropriately designed to mitigate identified risks; 3) controls are consistently executed and appropriately evidenced; and 4) higher-risk SOX controls are periodically tested.

Risk:

Potential that SOX controls are not adequately designed and effectively executed leading to financial misstatements not being prevented or timely detected.

key processes have been scheduled to assess the design of the associated control structures. The design gaps identified within this audit will be considered as part of the cycle's design assessment and updates to the control structure and descriptions will be made after the design assessment has been completed.

Additionally, the SOX team will continue to meet with the IT Compliance team on a weekly basis to ensure that any changes to IT controls do not negatively impact the associated business processes and to ensure risk management is assessed comprehensively for the business cycle.

Responsible:

Kristen King (SOX team)
Kimberly Jones (IT Compliance team)

Resolution Date:

October 2022

4) <u>Enhancing Controls Over Rate Update Access</u>		<u>Risk Rating:</u> 4
<u>Observation:</u> The ability to update billing rates in the customer information system is limited to those granted a specific access profile. Currently, this profile is granted through NiSource's standardized enterprise identity and access management solution, SailPoint IdentityIQ, upon the approval of the requesting employee's supervisor. If access was inappropriately approved, it would not be identified until the semi-annual access review is performed. We assessed the access review performed in second quarter of 2021 and noted that one employee incorrectly obtained rate update access after the wrong access profile was approved by the supervisor. The incorrect access was identified as part of a bi-annual access review performed by management in July 2021 and corrected subsequent to the review. While the customer information system does not have the capability to track whether actions were taken by the user with the incorrect access, mitigating controls are in place and operating effectively which would detect inappropriate changes to the billing rates. <u>Criteria:</u> Processes are sufficient to ensure that access to higher risk application functions and data is appropriate in accordance with users' roles and responsibilities, specifically access is granted based on both supervisor and data owner approval. <u>Risk:</u> Potential for inappropriate access to applications and data to result in unauthorized changes to business data.	A management response is not requested; however, management enhanced the rate update access profile provisioning process to include an additional level of approval within SailPoint IdentityIQ (performed by Regulatory department personnel) to ensure supervisor approvals are appropriate.	

***** End of Report*****



NiSource Gas Distribution

Operator Qualification Management

Internal Audit Advisory Report

Distribution

Beneficiaries

Sandra Brummitt	Daniel Creekmur	William Mojica
	David Monte	
	Marie Walker	

Other Key Personnel

Robert Heidorn	Adam Lanier	Daniel Norris
Troy Page	Timothy Parish	Michael Ray
	Jennifer Sawyers	
	Dana Willingham	

For Information

Shawn Anderson
Donald Brown
Kim Cuccia
Charles Shafer
Violet Sistovaris
Pablo Vegas
Lloyd Yates

Internal Audit Advisory Report

Background

NiSource Inc. (NiSource or the Company) operates six affiliated gas distribution companies across six states. Approximately 7,000 employees and contractors perform various activities to construct and maintain gas pipelines. The United States Department of Transportation (DOT) Pipeline and Hazardous Materials Safety Administration (PHMSA) has established a requirement that all gas technicians who perform specific activities on gas pipeline assets be adequately trained.

To comply with this requirement, NiSource has developed formal operator qualification (OQ) programs for each gas distribution company and established covered task listings to correlate specific construction and maintenance activities to associated training and qualification requirements. NiSource is transitioning to a common OQ framework, which will provide additional granularity in covered task definitions and strengthen qualification requirements. Additionally, in August of 2021, NiSource began migrating records maintained within the Learning Management System (LMS) application and the Industrial Training Services (ITS) Onboard application to the Energy WorldNet (EWN) application.

Audit Objective, Approach, and Coverage

The objective of this advisory assessment was to evaluate the effectiveness and efficiency of processes and controls associated with operator qualification activities. At the beginning of our audit, we completed a risk assessment, and we conducted detailed process assessments and records analysis in higher-risk areas. The review period for this audit was September 2021 through February 2022.

During our advisory assessment, we specifically evaluated:

- Program administration activities
- Operational execution activities, with a particular focus on the Quick Response (QR) card process
- Monitoring controls, including oversight of contractors, exception reporting processes and tracking and trending of identified instances of non-compliance
- Training and testing processes
- Change management activities

Summary of Key Internal Audit Recommendations

The advancement of a common OQ framework is driving consistency and will facilitate the ability to transfer qualified resources between operating companies. The new framework is also expected to optimize technicians' qualifications and performance by correlating qualifications and skills development with specific tasks that technicians perform related to their respective roles. However, under the new framework, the number of covered tasks has increased by approximately three times compared to the less granular legacy programs. The increase in covered tasks and addition of skills assessment requirements is expected to lengthen the time required for field personnel to complete training and assessment activities. Similarly, the skills assessment requirements will also increase the need for qualified evaluators. These changes coupled with decreasing average field personnel experience levels could lead to shortages of qualified field personnel. We recommend that management continue to evaluate and assess existing staffing and development activities to ensure resources needed to support the evaluation activities are sufficient and field personnel are adequately supported through OQ processes to successfully obtain qualification and return to their responsibilities.

The Company is improving OQ processes and records. However, due to limitations with the work management systems that NiSource currently uses, job order records do not specify which technicians completed particular tasks; as a result, the Company may not be able to fully evidence that covered tasks were completed by appropriately qualified individuals. As management looks long-term to its investment in new work management

technology, we recommend considering functionality that enhances traceability and enables task-level tracking, with specific focus on higher-risk activities where span of control, defined as the ratio of qualified versus unqualified individuals who can safely perform a covered task, would not apply.

During our review, we observed some opportunities to further enhance current and developing activities and controls. We discussed less-significant recommendations with management during our review, and a summary of our key recommendations follows:

1) OQ Non-Compliance Investigation Processes

If an instance of OQ non-compliance is identified, additional investigation of other work performed by the non-qualified personnel may be warranted to understand the extent of non-compliant work completed and impacted pipeline assets. Investigation processes and documentation requirements have not been formalized across the NiSource gas distribution companies. Lack of formal processes increases the risk of inconsistent or inadequate investigation procedures, inadequate investigation records, and insufficient remediation efforts.

We recommend that management continue their efforts to develop and formalize consistent processes to support investigation and remediation efforts associated with identified instances of OQ non-compliance, including definition of documentation requirements.

2) Controls over Qualification Records Creation and Changes

EWN is a Software as a Service (SaaS) application, meaning that while users access the application through the NiSource network, the application functionality is contained within the provider's network. NiSource employees and contractors may view their NiSource qualification records within the EWN application but should not have access to make changes to records, with the exception of approved users (e.g. NiSource OQ Project Specialists) who are granted application permissions to allow them to create and edit covered tasks and qualification records under NiSource's account. When a qualification record is created, the application should also be programmed to ensure all required information is captured. During a review of all contractor qualification records, key fields related to the name and company of the skills evaluator were not populated within seven records, resulting in the inability for NiSource to evidence that the associated individuals' qualifications were properly evaluated. As of the date of this report, EWN is investigating the cause of these errors.

We recommend that the NiSource OQ team partner with EWN to investigate the identified exceptions and ensure the application controls over the creation and submission of qualification records meets Company objectives and requirements. Additionally, management should ensure that relevant application controls, including security access controls, are periodically verified. Specifically, the organization should, periodically (at least annually) request and obtain the vendor's System and Organization Controls (SOC) assessment (SOC2 Type II) to ensure EWN's control environment is sufficient, controls are operating effectively, and defined user entity control responsibilities are effectively identified and managed by NiSource.

3) Monitoring over Qualification Processes

Although EWN captures key data points within submitted qualification records which can provide insight into the workforce's adherence to qualification processes and requirements (e.g. skill evaluators, exam proctors, test scores, exam attempts, exam dates and times), OQ Program Specialist are currently only able to view limited fields within individual qualification records and robust reporting has not been established, potentially limiting their ability to identify non-compliance, outliers or negative trends in process execution or process inconsistencies.

We recommend that NiSource continue to partner with EWN to develop reporting at individual, operating company, and at a full-company level for both employee and contractor populations which can enable better monitoring and oversight of adherence to OQ processes.

4) Third-Party Contractor Staffing Risk Management

Processes have not been established to ensure that individuals working for third-party contractors who have repeated process execution issues and/or repeated OQ violations are prevented from being engaged by a different third-party contractor to perform work on NiSource assets. As a result, an individual who may introduce process or compliance risk could be engaged to work on NiSource assets.

We recommend that NiSource design controls to ensure that individuals who have repeated process execution deficiencies and/or repeated OQ violations are not engaged to work on NiSource assets. Specifically, the Company should work with third-party contractors to ensure processes are sufficient to identify and screen out individuals that have had repeated problems with NiSource. Also, NiSource should ensure that the operating companies' hiring processes are sufficient to identify and screen out individuals that have had previous problems within NiSource.

5) OQ QR Card Processes:

The OQ QR cards have been implemented for employees and contractors across all six gas distribution companies and allow field personnel to access their own role qualifications in addition to required qualifications for specific field activities. Management is also in the process of incorporating references to Standard Operating Procedures (SOPs), enabling field personnel to access further detail on proper operational execution of field activities.

Currently, field personnel reviewing information displayed on their OQ QR card in combination with the responsible supervisor's oversight are the key controls established to ensure non-qualified personnel abstain from completing covered tasks; however, the ability of field personnel to easily access and digest the necessary information may be impacted by their device capabilities (e.g. screen size, connectivity, etc.). Misunderstanding one's OQ status may lead to work being performed by unqualified personnel.

We recommend that management continue to utilize feedback obtained from surveys of the frontline workforce on their experience and the "user-friendliness" of the in-field system to identify ways to provide the necessary information in the most convenient and digestible way possible. Additionally, given the execution of these established controls is distributed given the large number of employees and contractors completing various activities in the field daily, the likelihood of non-compliance increases. Ideally, a technology solution could be created and implemented that integrates work planning and scheduling with OQ to provide visibility in the assigning process to ensure properly trained and qualified personnel are assigned to complete qualified tasks.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Advisory Report *****

NiSource Inc.

Management of Change Advisory Review

Internal Audit Advisory Report

Distribution

Beneficiaries

Dave Monte
Charles Shafer

Other Key Personnel

Lauren Anderson

For Information

Shawn Anderson
Melanie Berman
Melody Birmingham
Donald Brown
Kim Cuccia
Bill Jefferson
Pablo Vegas
Lloyd Yates

Background

NiSource Inc. (NiSource or the Company) has implemented a formal Management of Change (MoC) program and associated tools as part of the Company's Safety Management System (SMS). Implementation of a MoC program is specified in American Petroleum Institute Recommended Practice 1173 (API RP 1173) and is a systematic approach to anticipate, identify, assess and control potential hazards and risks associated with changes before they are rolled out. NiSource uses the DevonWay, Inc. (DevonWay) application MoC module to process and manage MoC submissions.

The Company's MoC team is a part of the SMS Central Support organization and engages with MoC initiators, the MoC Committee, and leaders throughout the Company to 1) ensure that change risks are identified, 2) monitor implementation plans and 3) identify continuous improvement opportunities. As of the time of this review, more than one hundred MoC initiatives had been submitted for evaluation.

Audit Objective, Approach, and Coverage

The objective of this advisory assessment was to provide an independent evaluation on the effectiveness and efficiency of the MoC process. Key review areas of this assessment included: the MoC submission and review process, defined roles and responsibilities, communication processes, training activities and outreach plans, and DevonWay application access.

During the advisory assessment, we specifically evaluated:

- Processes to ensure proper oversight over physical, procedural organizational and technological changes
- Governance processes and established roles and responsibilities outlined in the SMS MoC program document
- Communication, training and outreach plans related to the MoC process
- Organizational adherence to the MoC program document
- DevonWay application access controls

We did not evaluate some programs that include MoC elements as described in Exhibit A of the MoC program document ("Processes Related to Management of Change") such as Transmission Integrity Management Programs (TIMP), Distribution Integrity Management Program (DIMP) and Standards Evaluation & Approval System (SEAS). These processes will be considered during future audit engagements.

Summary of Key Internal Audit Recommendations

The MoC team has developed a procedure and executed initial communication and training plans. As part of our evaluation process, we interviewed a cross section of stakeholders impacted by MoC processes. The launch of the MoC program has been generally successful. Personnel impacted by the Blackline Personal Protection Device (Blackline) rollout were especially complimentary of the MoC approach, which facilitated effective collaboration and engagement across the impacted groups. Also, the NiSource leaders that we interviewed support the MoC process and described the MoC team as responsive and accessible.

To facilitate awareness and adoption of the process, the MoC team should continue to promote the MoC process with regularly scheduled communication and training campaigns. While we found that affected employees are aware of the MoC process, management should provide further instruction on the scope of this operationally focused procedure and clarify when to use this process versus other change management processes. Additionally, to ensure that the MoC process remains effective and aligned with the Company's change environment, management should periodically evaluate the MoC procedure and calibrate the MoC review questionnaire.

During our review, we observed some opportunities to further enhance current and developing activities and controls. We discussed less-significant recommendations with management during our review, and a summary of our key recommendations follows:

1) Assessment of External Change Risk Factors

The objective of the MoC process is to ensure that changes impacting NiSource are identified and managed. The MoC request form is intended to capture information relevant to identifying risk associated with a change. The current form being used by NiSource is closely aligned with API RP 1173 and primarily focuses on factors internal to a Company. The form is not customized in consideration of NiSource's culture, circumstances and objectives. Also, the form does not directly address potential for public safety incidents or customer impacts. As a result, risk assessment processes may not identify all (internal and external) risk factors, which could impair risk management processes.

We recommend explicitly including external risks factors such as public safety and customer impacts on the MoC review request form to ensure that information relevant to managing external risks are captured and considered in the risk evaluation process. Also, management should consider if other changes to the MoC program document are warranted based on the Company's particular culture, circumstances and objectives.

2) Alignment with API RP 1173

API RP 1173 specifies that the MoC process shall consider both permanent and temporary changes. While NiSource's MoC program document specifies that changes can be either permanent or temporary, all MoC submissions as of the time of our review related to permanent changes. Additionally, API RP 1173 specifies communication to contractors must occur when those contractors can be affected by the change. While the Company's MoC program document requires that impact on contractor procedures be considered, the responsibility to communicate changes to contractors is not clearly defined. Failure to clearly define roles and responsibilities for communicating changes to contractors could result in inconsistent communication leading to improper implementation of changes and/or insufficient management of change risks.

We recommend that the MoC program document be expanded to define roles and responsibilities for communication of changes to contractors. Also, as a component of communication and training campaigns, the MoC team should emphasize that temporary changes are expected to be assessed to the same standard as permanent changes. The program document does not provide actions or expectations regarding changes that are temporary in nature. We recommend providing additional information in the program document to facilitate application of the process in the NiSource environment for temporary changes.

3) MoC Initiative Committee Review

All committee members review all the submitted initiatives, including those outside their areas of subject matter expertise. While the MoC process has been initially focused on gas operations activities, the process is intended to be scalable. However, representatives for some functions (e.g., Customer Service and Generation) are not included on the MoC Committee.

To facilitate efficiency and effectiveness, the MoC team should consider restructuring committee review processes to focus committee members' participation based on their expertise relative to each change and associated potential risks.

4) Best Practices and Lessons Learned Knowledge Transfer Process

While best practices and lessons learned are informally reviewed and discussed at various MoC meetings, this knowledge is not always formally captured and communicated. Formally capturing and communicating best practices and lessons learned facilitates knowledge transfer and promotes efficiency and effectiveness.

We recommend that the MoC team formalize processes related to discussing and capturing best practices and lessons learned, which will enhance process consistency, promote efficiency, and enable knowledge transfer when onboarding new employees, MoC committee members and MoC initiators.

5) Implementation of Changes

While various organizations consider the timing of changes impacting the field personnel, the MoC committee does not formally evaluate the timing and sequence of changes. As a result, compounded risk related to multiple changes, especially multiple changes impacting the same areas, may not be fully recognized and appropriately managed through the MoC process.

We recommend the MoC team formally consider compounded risk related to multiple changes and formally consider the timing and sequencing of changes. The MoC team should continue to work with other organizational teams to streamline the pace of change and minimize the potential for adverse events.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Advisory Report *****

NiSource Inc.

Environmental Data Quality and Reporting Controls

Internal Audit Advisory Report

Distribution

Beneficiaries

Valarie Bomar

Kelly Carmichael
Gunnar Gode

Daniel Creekmur

Other Key Personnel

Stephen Holcomb

Kristen King

Margaret Rice

For Information

Shawn Anderson
Melanie Berman
Melody Birmingham
Donald Brown
Kimberly Cuccia
William Jefferson
Lloyd Yates

Internal Audit Advisory Report

Background

NiSource Inc. (NiSource) is committed to delivering energy safely, reliably and in an environmentally responsible and sustainable way while maintaining compliance with federal, state, and local environmental regulations. As part of an ongoing initiative to provide transparency related to sustainability progress, NiSource discloses a variety of environmental information to investors. These disclosures include qualitative information and quantitative metrics associated with portfolio data, emissions, and natural resources. Reporting has come under increased scrutiny, and the U.S. Securities and Exchange Commission (SEC) issued a proposal in March 2022 that would require public companies to disclose specified climate-related information in certain filings. Additionally, in May 2022, the SEC proposed two form and rule amendments seeking to enhance and standardize certain environmental, social and governance (ESG) disclosures related to funds and advisers.

The NiSource Environmental team is responsible for coordinating with data owners across NiSource to obtain the data inputs necessary to compile and produce environmental reporting information. At the time of our review, environmental reporting activities were completed and tracked manually, but the team was in the process of implementing the Workiva ESG reporting platform (Workiva). The team has subsequently made the decision to transition from Workiva to a different data collection and collaboration tool.

Audit Objective, Approach, and Coverage

The objective of this advisory assessment was to provide an independent evaluation on the effectiveness and efficiency of controls related to environmental data quality and reporting. At the beginning of our audit, we completed a risk assessment, and we conducted detailed process assessments and selection testing in higher-risk areas, specifically processes and controls associated with the greenhouse gas (GHG) emissions metric. The review covered processes in place at the time of the audit.

During this advisory engagement, we assessed the design of processes and controls associated with data quality and reporting and specifically evaluated the following:

- Risk assessment processes
- Adequacy of policies and procedures around metric definitions, calculations, estimates/assumptions, and methodologies
- Data management activities, including data ownership definitions, collection, data quality and review processes, and organization and access management
- Review and governance activities
- Metric consolidation and disclosure activities

We did not evaluate information technology general computer controls or access security as the technology implementation was ongoing at the time of our review.

Summary of Key Internal Audit Recommendations

The Environmental and Financial Reporting teams continue to stay apprised with the progress of the proposed SEC rule changes, and the Environmental team is actively working to implement process improvements. Implementation of a data collection and collaboration tool offers the opportunity to implement preventative application controls that facilitate data integrity and efficiency through automation of data requests and notifications. We recommend that management strive to automate controls as much as possible to enhance the consistency of the control environment.

During this advisory review, we observed some opportunities to further enhance current and developing activities and controls. We discussed less-significant recommendations with management during our review, and a summary of our key recommendations follows:

1) Definition of ESG Reporting Internal Control – Integrated Framework Accountabilities and Responsibilities

The Environmental team is focused on implementing data and process controls for which the Environmental team has direct responsibility. However, NiSource has not officially begun or defined which organization/function should be accountable and responsible for scoping, defining, implementing, and maintaining an overall program designed to provide reasonable assurance regarding the achievement of objectives and oversight of internal control systems relating to ESG reporting (i.e., a program to establish and then maintain an internal control - integrated framework for ESG reporting).

Implementation of an internal control - integrated framework, such as the framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), provides external and internal stakeholders with greater confidence in achievement of objectives and oversight of internal control systems. Further, implementation a framework such as COSO provides an opportunity to eliminate ineffective, redundant, or inefficient controls. We recommend that NiSource management officially define which organization/function should own the implementation and then maintenance of an internal control - integrated framework for ESG reporting and ensure that sufficient resources are allocated to the implementation initiative and ongoing program. We specifically recommend implementing a COSO Internal Controls – Integrated Framework structure, which is the framework that management has adopted for internal control over financial reporting.

2) Incomplete Standard Operating Procedures

While certain components of environmental reporting activities are documented, standard operating procedures detailing key steps related to data compilation, metric calculations, and reporting processes are not maintained. We evaluated the procedural documentation for the GHG emissions metric and noted that, while a listing of data inputs associated with the responsible data owners is maintained, data compilation and calculation procedures are not documented. Additionally, some data owner information is outdated.

Standard operating procedures facilitate execution consistency, verification activities, and knowledge transfer. We recommend that management develop standard operating procedures for each key metric and disclosure, including a definition of data inputs and the associated data owners, calculation procedures, compilation processes, and required verification activities. Additionally, management should define change management processes, including a process to periodically review and validate the accuracy of standard operating procedures.

3) Controls over the Completeness and Accuracy of Data Used to Calculate Metrics

The Environmental team uses data submitted by multiple data owners to calculate metrics, and controls to ensure the completeness and accuracy of these data inputs are not formalized and documented. Specifically:

- Data inputs are not reconciled to source information
- Parameters for system generated reports are not periodically verified
- Review controls are not formalized to evidence data verification or management's oversight

Insufficient control over data inputs increases the potential that metric calculations will be incorrect, and metrics will be inaccurately reported. We recommend that management establish and document controls that ensure the completeness and accuracy of data used as inputs to metric calculations. The Environmental team and data owners should establish data submission processes that include steps to verify or review the reasonableness of data that is used to calculate metrics.

4) Information Technology General Computer Controls for Materially Significant Systems

Data used in environmental metric calculations or disclosures originate from several sources and may be processed or stored in various technological solutions. A population of technology platforms,

databases, and applications materially significant for the calculation of environmental metrics has not been formally identified and documented, and information technology general computer controls for the associated systems may not have been evaluated and may be inadequate. For example, a materially significant data input to the GHG metric originates from the Continuous Emissions Monitoring System, and access to this web-based application is not periodically reviewed and other information technology general computer controls have not been validated.

Inadequate information technology general computer controls may result in the integrity, availability, or confidentiality of data being compromised. Management should compile an inventory of the applications relevant and materially significant to environmental metric calculations and disclosure reporting and ensure that general computer controls are appropriate to maintain the integrity and availability of data.

5) Controls to Ensure the Integrity of Management Estimates

Management estimates are a key data input for some environmental metric calculations. Errors of assumptions or other factors in management's estimates could impact the accuracy of a reported environmental metric. The risk of a material error varies with the number and significance of assumptions made and the degree of uncertainty associated with the assumptions. The GHG metric includes a key data input that is based on management estimates. The estimated data we reviewed was well-supported, with thorough documentation of the assumptions and factors utilized, including documentation of management's review and approval of the assumptions and factors utilized. However, the full population of estimates included in all reported metrics has not been formally documented and risk assessed, with associated assumptions for management's higher risk estimates validated.

We recommend that management formally identify the population of management estimates included as key data inputs to reported metrics. For each estimate utilized, management should identify the relevant factors and assumptions used in the estimate and ensure formal procedural documentation is developed outlining calculation steps, assumptions that represent management's judgement, and the associated management review controls performed to validate the estimate. Additionally, processes should be implemented to periodically reassess the relevance of key management estimates and verify the design of associated management review controls.

6) Data Inputs Provided by Third Parties

Some environmental metric calculations include data inputs that are provided to NiSource by third parties. A process to verify that the third parties' internal controls are operating effectively is not established. Three data inputs for the GHG emissions metric calculation are provided by third parties, and the internal control environments for these third parties have not been verified by NiSource. While these data inputs to the GHG emissions calculation do not introduce a significant risk for a material error to the reported metric, the full population of data originating from third parties that are utilized across all metric calculations has not been formally documented and risk assessed.

Inadequate internal controls could impede third parties from providing accurate and complete information to NiSource, and, therefore, prevent NiSource from timely reporting accurate environmental metrics. We recommend that management assess the materiality and impact of all third-party data inputs utilized in environmental metric calculations and ensure that internal controls are periodically assessed for significant third parties. Specifically, the organization should periodically (at least annually) request and obtain System and Organization Controls (SOC) assessment reports (SOC2 Type II) for all significant third parties to ensure the third parties' control environments are sufficient and controls are operating effectively. Additionally, associated user entity control considerations should be identified and evaluated for effectiveness by NiSource.

7) Management Analysis of Fluctuations in Calculated Metrics

Processes to evaluate period-over-period fluctuations in calculated metrics are not formalized. While the Environmental team completes a year-over-year comparison of the GHG emissions metric, a formal

review process that includes a thorough analysis of fluctuations against established variance thresholds is not performed.

Informal and/or insufficient management review and analysis procedures could lead to unexplained variances outside of the organization's risk tolerance not being detected and investigated. We recommend that management implement formal period-over-period fluctuation analysis procedures. The analysis should be performed against established variance thresholds that are appropriate in consideration of the organization's reporting risk tolerance. Also, reviews should be performed by knowledgeable personnel at an appropriate organizational level and formally evidenced.

8) Data Security Controls for Information Stored on Shared Network Drives

The shared network drive utilized by the Environmental team to store and manage all environmental data input source files and calculation files lacks certain security controls to ensure the data is complete and accurate. While access to the network drive is managed through the Company's identity and access management tool, members of the Environmental team who are not responsible for environmental reporting also have access to the drive, and key files are not password protected and processes have not been established to manage version control risk.

Inadequate control over data files relevant to calculating and reporting environmental metrics could result in data integrity being inadvertently or intentionally compromised, which increases the risk of environmental metrics not being timely and accurately reported. The Environmental team noted that implementing a data collection and collaboration tool should allow for additional functionality to restrict edits to data saved within the tool based on user permissions. We recommend the Environmental team implement interim controls (e.g., password protecting folders or files on the shared drive to restrict access to appropriate users) until full utilization of a technology tool is realized. Additionally, we recommend establishing a process to lock finalized files to prevent final data from being edited.

9) Governance and Knowledge Transfer

The Environmental team compiles multiple metrics, disclosures, and formal reports on behalf of the Company. A full inventory of information that is reported, including the method of reporting and the associated timelines, is not documented, which increases the potential for missed or delayed reporting.

We recommend establishing an overall checklist encompassing the metrics and reporting to be submitted that includes the name of the preparer, reviewer, submitter, and related due date.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Advisory Report*****

Columbia Gas Distribution Companies

Manual Billing Processes

Internal Audit Report

Distribution

Respondents

Angela Sanchez
Jennifer Shikany

Beneficiaries

Michele Caddell

Dan Douglas

Jennifer Montague

Other Key Personnel

Heather Bauer
Gunnar Gode
Kristen King

For Information

Shawn Anderson
Melanie Berman
Donald Brown
Melody Birmingham
Kimberly Cuccia
William Jefferson
Lloyd Yates

Internal Audit Report

Background

The Columbia Gas Distribution Companies (CGC or Columbia Gas), which is comprised of five natural gas distribution subsidiaries fully owned by NiSource Inc. (NiSource or “the Company”), deliver natural gas to approximately 8,000 gas measurement billing (GMB) customers, which are determined based on their gas pressure, gas needs, and metering equipment. Most (approximately 85%) large volume customers purchase natural gas from a certified supplier and participate in the gas transportation service (GTS) program. Other large volume customers purchase natural gas from Columbia Gas and are referred to as GMB sales customers. The amount billed to large volume customers totaled \$175.3 million in 2021 and \$116.4 million through the second quarter of 2022, of which \$156.8 million and \$98.8 million, respectively, was billed to GTS customers.

Billing rates for GMB sales and GTS customers are defined in commission-approved tariffs and are dependent upon consumption. A specialized team within the CGC billing group manages billing, including meter reading, and tariff compliance monitoring activities for large volume customers. Bills for GTS customers are generated using the GTS billing system while bills for GMB sales customers are generated from the CGC Distributive Information System (DIS) customer billing system.

Audit Objective, Approach, and Coverage

The objective of this risk-based internal audit was to provide an independent evaluation of the adequacy, effectiveness, and efficiency of controls associated with manual customer billing for the Columbia Gas Companies. At the beginning of our audit, we completed a risk assessment, and we conducted detailed process assessments and sample-based transactional testing in higher-risk areas. We tested transactions related to the period between February 1, 2021, through January 1, 2022.

During the audit, we specifically evaluated processes and controls related to:

- Tariff and contract compliance
- Billing completeness and accuracy
- Billing exceptions and adjustments activities
- Billing systems data security (specifically, system access controls)

We did not evaluate processes and controls related to gas supply, which will be audited separately.

Internal Audit Finding Ratings

We assign ratings to audit findings based on the following scale (see the Internal Audit Finding Rating Scale in Appendix A):

“1” – Significant Improvement is Needed and Prompt Management Attention is Required

“2” – Improvement is Needed and Management Attention is Necessary

“3” – Some Improvement is Needed and Management Attention is Justified

“4” – Management Evaluation is Desirable

Internal Audit Conclusion and Summary of Observations

NiSource employees responsible for the execution of manual billing processes have extensive experience and insight into these processes. However, we observed that the processes to ensure large volume customer billing is

complete and accurate are reliant upon the knowledge and expertise of the responsible employees as opposed to an adequately designed and effectively executed control framework. We recommend that management formalize oversight and monitoring controls to ensure accurate billing and facilitate execution consistency and knowledge transfer.

Overall, we found that processes and controls related to manual billing processes (as specified in the "Audit Objective, Approach, and Coverage section of this report) were generally operating as intended. We did, however, identify two findings where management's attention is necessary (Rating 2). In addition, we observed some less-significant items that were discussed with management during the audit.

A summary of audit findings rated "1" through "3" follows (see the Internal Audit Findings Matrix in Appendix B):

- 1) Large Volume Customer Billing System Tariff Rate Change Controls (Rating 2)
Controls and processes are insufficient to ensure large volume customer tariff rate changes resulting from the annual consumption review are timely processed in the appropriate billing system.
- 2) GTS Customer Unbilled Customer Usage Controls (Rating 2)
Controls and processes are insufficient to ensure that all GTS customer usage is accurately billed.

Management's Response

Management agrees with the findings noted during this audit and has provided action plans to address the risks identified. Detailed action plans are included in Appendix B. The key mitigation steps will be completed by August 2023.

Internal Audit Follow Up

Management has provided action plans for all findings with a rating of "1", "2", or "3". We have reviewed management's action plans and believe that the action plans will adequately address the findings identified in this audit. We will track the progress of resolution and will conduct follow-up testing for all rated "1" audit findings and a sample of rated "2" and rated "3" audit findings.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Report *****

“1” Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company’s reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

“2” Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

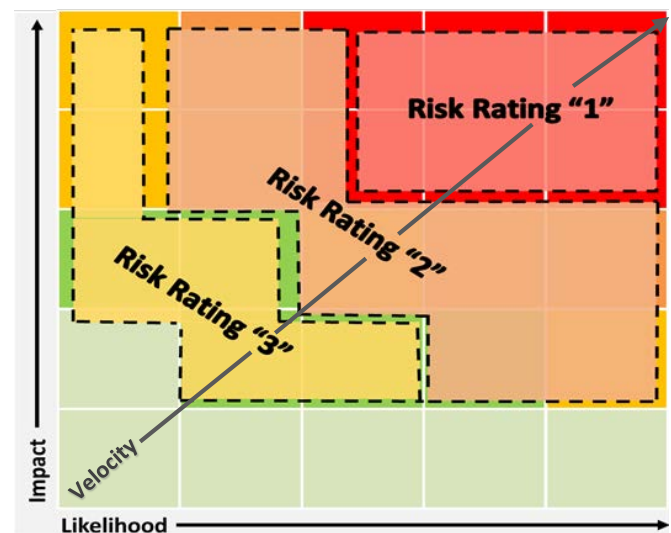
- More than remote probability for damage to the Company’s reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

“3” Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

“4” Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited



1) Large Volume Customer Billing System Tariff Rate Change Controls

Risk Rating: 2

Observation:

To ensure that large volume customer tariff rates are appropriately applied consistent with consumption per the regulator-approved customer tariffs, the Regulatory Studies team performs an analysis of large volume customer consumption annually for all Columbia Gas Distribution Companies (CGC), except Kentucky, and communicates required tariff rate changes to the Billing team. However, gas measurement billing (GMB) sales and gas transportation service (GTS) customer tariff rate changes must be manually processed in the respective billings systems by the Billing team, and processes and controls are not sufficient to ensure that tariff rate changes are timely processed; specifically:

- Tariff rate changes for five large volume customers related to the 2021 consumption analysis were not processed in the respective billing systems until September 2022 resulting in underbilling customers approximately \$82,000 and overbilling customers approximately \$67,000 (net revenue impact of approximately -\$15,000)
- Decisions to retain system tariff rates inconsistent with the results of the annual customer consumption analysis are not formally documented and approved

Criteria:

Controls are sufficient to ensure that large volume customer tariff rates are appropriately applied consistent with consumption per the regulator-approved customer tariffs; specifically: 1) large volume customer consumption is formally analyzed relative to approved tariff parameters; 2) processes to change tariff rate parameters in billing systems are formalized; 3) the duties of requesting, processing, and validating billing system tariff rate changes are appropriately segregated; 4) changes resulting from the annual customer consumption analysis occur at a formally-specified time and execution of the process is confirmed; and 5) decisions to retain system tariff rates inconsistent with the regulator-approved tariffs are formally documented and appropriately approved.

Management Action Plan:

NiSource GTS and Transportation Sales Support (TSS) and Regulatory Studies management has completed the following actions:

- Review the updated GMB and GTS annual consumption review process with the Billing team and perform targeted training as necessary

NiSource GTS and TSS and Regulatory Studies management will complete the following actions:

- Formalize a process to confirm timely execution of the tariff rate changes in the billing systems by another member of the Billing team, including positive verification the rates have been updated in GTS as well as the effective date of the changes
- Formally document and approve decisions to retain system tariff rates inconsistent with the regulator-approved tariffs

Responsible:

Angela Sanchez, Director Gas Transportation Program / C&I Billing
Jennifer Shikany, Director Regulatory & Utility Optimization

Resolution Date:

Regulatory Studies conducted the updated annual GMB and GTS consumption analysis process review with the Billing team in September 2022.

The 2022 consumption review process was updated in September 2022 inclusive of the changes outlined above. The noted action steps will be completed by January 2023 for the Ohio, Pennsylvania, and Maryland reviews and by August 2023 for the Virginia review.

<u>Risk:</u> Customers are incorrectly billed resulting in revenue being incorrectly recorded and negative reputational impact with customers and regulators.	
2) <u>GTS Customer Unbilled Customer Usage Controls</u>	<u>Risk Rating: 2</u>
<u>Observation:</u> In January 2022, the Regulatory Studies team identified one GTS customer with natural gas usage that was unbilled for April and May 2021 (totaling approximately \$12,000) through rate case revenue analysis. Controls and processes to ensure that all GTS customer usage is accurately billed to customers are insufficient; specifically: • Current processes to reconcile customer accounts which are flagged as GTS in the Distributive Information System (DIS) to those recorded in the GTS billing system each cycle are not sufficient to ensure all GTS customers with usage are billed and is subject to manual error • Technology or process controls do not prevent GTS billing system customer account changes from occurring without proper authorization (e.g., a workflow approval step) • GTS billing system customer account changes are not monitored <u>Criteria:</u> Controls and processes are sufficient to ensure that all GTS customer usage is accurately billed; specifically: 1) access to change customer accounts in the GTS billing system is restricted; 2) technology or process controls prevent customer account changes from being implemented without proper authorization; 3) customer account changes are monitored; 4) GTS billing system customer accounts are reconciled to DIS customers flagged as GTS; and 5) all large unbilled usage is monitored.	<u>Management Action Plan:</u> GTS and TSS management investigated restricting access to change customer accounts within the GTS billing system to a limited number of users; however, due to system role definitions and required job responsibilities, it is not currently possible to further restrict system access. GTS and TSS management also explored formalizing a process to periodically monitor all GTS customer account changes. However, approximately 21,000 account changes (e.g., customer additions, deletions, contract processing) are processed annually and there is currently no reporting to isolate customer additions and deletions. Additionally, there are existing controls in place to ensure customer billing adjustments are appropriate. GTS and TSS management will enhance controls and ensure that all GTS customer usage is billed by developing and implementing a query to reconcile accounts with natural gas usage in DIS coded as GTS against accounts within the GTS system prior to the start of each month's billing cycle. Identified discrepancies will be investigated and resolved within the billing cycle. <u>Responsible:</u> Angela Sanchez, Director Gas Transportation Program / C&I Billing <u>Resolution Date:</u> The action step noted above will be completed by April 2023.

<u>Risk:</u> Customers are incorrectly billed resulting in revenue being incorrectly recorded and negative reputational impact with customers and regulators.	
3) <u>Meter Data Accuracy Review Testing Procedures</u>	<u>Risk Rating: 4</u>
<u>Observation:</u> Approximately 13% of total GMB and GTS customers utilize meters which measure volume on paper charts, and the consumption reads from these charts are manually entered into DIS before customer bills can be generated. While there is an established Sarbanes-Oxley (SOX) control to ensure consumption per the paper charts is accurately entered into DIS, the related SOX testing validation procedures do not require the tester to verify the accuracy of the meter volumetric data entered from the paper charts into the billing system. As a result, the SOX validation testing does not fully assess control execution effectiveness and ineffective control execution may not be identified. <u>Criteria:</u> SOX testing procedures are sufficient to identify ineffective control execution; specifically: test procedures include 1) validation that the chart information agrees to the volume recorded within DIS; and 2) verification that the chart to DIS comparison was initialed by the associate reviewing the chart. <u>Risk:</u> Potential that ineffective control execution is not detected leading to a control issue going unresolved and customers being incorrectly billed resulting in revenue being incorrectly recorded and negative reputational impact with customers and regulators.	A management response is not requested; however, Internal Audit recommends that management enhance the current SOX control testing procedures by adding test steps to validate that the paper chart information agrees to the volume recorded within DIS.

***** End of Report*****

NiSource Inc.

Gas Standards Management Advisory Review

Internal Audit Advisory Report

Distribution

Beneficiaries

Paul Hunter

William Mojica

Steven Sylvester

Other Key Personnel

Eric Belle

Adam Lanier

Donald Reynolds

For Information

Shawn Anderson

Melanie Berman

Melody Birmingham

Donald Brown

Kim Cuccia

William Jefferson

Lloyd Yates

Internal Audit Advisory Report

Background

NiSource Inc. (NiSource or the Company) operates six affiliated gas distribution companies across six states. To facilitate consistent operational execution and adhere to various compliance requirements, a centralized Gas Standards team develops and administers formalized policies and procedures (referred to herein as “gas standards”) that cover asset construction, operations, and maintenance activities for gas transmission, distribution, and underground storage facilities. The team is comprised of 13 employees and is supplemented by third-party contractors as needed.

To administer requests for the development of new gas standards or revision or reaffirmation of existing gas standards, the Gas Standards team currently utilizes a web-based collaborative platform tool, referred to as the Standards Evaluation & Approval System (SEAS). At the time of our review, 547 gas standards, 46 operational notices (i.e., official directives pending issuance of a formal gas standard) and 80 associated forms, checklists or tags were published and active across the six gas distribution companies. In October 2021, the Gas Standards team published a gas standard titled “Periodic Maintenance of Gas Standards” which formalized requirements to review gas standards every five years and take action to revise, reaffirm or cancel gas standards to ensure they do not become outdated or include non-applicable operational processes.

Audit Objective, Approach, and Coverage

The objective of this advisory assessment was to provide independent recommendations on the effectiveness and efficiency of processes and controls associated with Gas Standards management activities.

During the advisory assessment, we specifically reviewed:

- Adequacy of policies and procedures
- SEAS application functionality and data capture
- Gas standards evaluation, development, revision, and reaffirmation activities
- Change management activities associated with gas standards updates, with specific focus on communication of changes to Company employees and third-party contractors

We did not perform a technical review of published gas standards in relation to regulatory requirements or engineering best practices. Additionally, we did not assess responsibilities of the Gas Standards team unrelated to gas standards (e.g., facility failure analysis, materials and equipment assessments, etc.).

Summary of Key Internal Audit Recommendations

The NiSource Gas Standards team is comprised of employees who have significant experience within the Company and on the team. However, the team has not formally benchmarked their processes and performance relative to similar organizations in peer gas distribution companies. While the Gas Standards team has significant technical expertise combined with a broad understanding of operational activities across the Company’s gas distribution affiliates, performing formal benchmarking may provide valuable insight regarding process optimization and resource allocation.

During our review, we observed some opportunities to further enhance current and developing activities and controls. We discussed less-significant recommendations with management during our review, and a summary of our key recommendations follows:

1) Alignment of Gas Standards Processes and Resources to Support Objectives

The number of SEAS requests is increasing year over year, and the average number of submitted SEAS requests submitted between 2019 and 2021 exceeded the average number of published gas standards by over threefold, with the gap between requests and number of standards published increasing each year. At the time of our review, 691 SEAS requests were active in various stages of the evaluation and development process, and almost 70% of these requests were aged more than a year.

Further, almost 40 percent of the active operational notices, which are intended to provide temporary guidance until gas standards can be finalized, were active for more than five years and several have been active more than 10 years, with the oldest outstanding for 18 years. Additionally, the new requirement to periodically review existing gas standards will compound the workload of the team who must already balance responsibilities for other activities related to but separate from gas standards (e.g., facility failure analysis, materials and equipment assessments, etc.). Given ongoing backlogs and the organization's objectives, current processes combined with the standing resource allocation are not sufficient to support the Company's growing gas standards administration needs.

Failure to resolve backlogs and manage processes and resources in a manner that enables timely development of gas standards increases operational and compliance risk. While additional contract resources can be engaged to help navigate workflow peaks and optimize cost efficiency, we recommend that the Company evaluate current processes and the resources allocation model to ensure alignment with the Company's objectives and risk tolerance.

2) Gas Standards Change Request Risk Assessment and Workflow Prioritization Processes

Anyone within the Company can request that a gas standard be created or evaluated by entering a request in SEAS. The Gas Standards team uses information provided by requesters (specifically, request driver category and desired effective date) to prioritize work. While the desired effective date is used to determine urgency of requests and the request driver category is anecdotally used to navigate workload according to risk, a quantitatively driven risk analysis process that drives an illustratable and consistent risk-based workflow approach has not been formalized. Also, workflow prioritization decisions are not always adequately evidenced.

Informal processes may result in inefficiency and inconsistency that impairs risk management and increases the costs associated with administering the Company's gas standards. We recommend the Gas Standards team design a formalized risk analysis process that is quantified as much as possible. Specifically, consider quantifying the comparative risk associated with the request driver categories. Also, consider what other quantifiable information is or can be captured and comparatively analyzed. Finally, the team should evidence risk-based prioritization decisions, which will facilitate process evolution and knowledge transfer.

3) Gas Standards Change Communication and Acknowledgement Processes with Vendors

The Gas Standards team distributes a monthly email to Company leaders communicating recently approved and published changes to gas standards. While the team historically communicated changes to impacted vendors and managed a process to verify vendors' acknowledgement of gas standard changes, these communication and acknowledgement activities are inconsistently executed, and the Company did not make a formal decision to suspend these processes. The most recent communication sent by the Gas Standards team to formally notify third-party contractors of NiSource gas standard changes occurred in October 2020. At least 160 SEAS requests have since been published.

While NiSource has recently established the Performance Support Tool, which enables employees and contractors to access current gas standards while in the field, and all field personnel are required to comply with the daily acknowledgement process (which directs field personnel to reference current gas standards prior to executing work), suspending change communication and change acknowledgement processes, without formally obtaining input from the Legal and Contractor Performance Management teams may increase risk to NiSource. We recommend that the Gas Standards team, in coordination with the Legal department and the Contractor Performance Management team, assess the cost versus benefit of formally managing a gas standard change communication and change acknowledgement process for third-party vendors.

4) SEAS Data Accuracy and Completeness

The Gas Standards team manually updates status information within the SEAS request records. Status information in SEAS is not always timely updated and certain key information is inconsistently recorded; specifically:

- SEAS request records do not always accurately reflect the status of the request, which may impair monitoring activities
- Information specific to interrelated processes, such as Corrective Action Plan (CAP) and Management of Change (MoC), is captured in free-form text fields (versus designated data fields), which impairs searching and analysis capabilities
- The date of and reason for the voiding or rejecting a submitted request is inconsistently populated within the application, which may impair the ability to verify information, knowledge transfer and process evolution
- A new date is not captured in SEAS when a request record transitions to a new status category, which impairs the ability to analyze cycle times and identify delays

We recommend that SEAS request record status is timely updated and key data elements are consistently populated. Consider implementing edit controls in SEAS that provide appropriate error messages and prevent the fields from being blank. Also, consider adding additional data fields for interrelated processes (specifically, CAP and MoC) to facilitate alignment with these requirements. Automated data interfaces to the technology platforms supporting the CAP and MoC processes may be beneficial in facilitating consistency, analysis and efficiency.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Advisory Report *****

NiSource Inc.

**Pipeline and Hazardous Materials Safety Administration
(PHMSA) Mega Rule**

Internal Audit Report

Distribution

Respondents

Aaron Boeke
Benjamin Turner

Beneficiaries

Sandra Brummitt	Robert Heidorn	William Mojica
	James Zucal	

Other Key Personnel

Katherine Creef
Jonathan Devries

For Information

Shawn Anderson
Melanie Berman
Donald Brown
Melody Birmingham
Kimberly Cuccia
William Jefferson
Lloyd Yates

Internal Audit Report

Background

NiSource Inc. (NiSource or the Company) serves approximately 3.6 million gas customers across six states and owns approximately 1,000 miles of transmission pipeline which are subject to the Pipeline and Hazardous Materials Safety Administration's (PHMSA) federal code requirements. In October of 2019, PHMSA released one part of a three-part ruling, collectively known as the Mega Rule, as a set of regulations strengthening requirements related to onshore gas transmission pipeline assets to improve pipeline safety by reducing the frequency of pipeline failures.

The first part of the Mega Rule became effective as of July 1, 2020 and focused on requirements for operators to verify that new, replaced, abandoned, or repaired steel transmission pipeline assets met traceable, verifiable, and complete (TVC) records criteria (as defined in the rule) and required the reconfirmation of the maximum allowable operating pressure (MAOP) and verification of material properties for any existing non-TVC transmission assets over a period of time, with 50 percent of applicable pipeline mileage required to be complete by July 3, 2028 and 100 percent by July 2, 2035.

Audit Objective, Approach, and Coverage

The objective of this risk-based internal audit was to provide an independent evaluation of the adequacy, effectiveness, and efficiency of processes and controls established to comply with the requirements of the first part of the PHMSA Mega Rule. At the beginning of our audit, we completed a risk assessment, and we conducted detailed process assessments and sample-based transactional testing in higher-risk areas. The review period for this audit assessed processes and controls in place as of October 2022 and transmission asset populations installed both pre and post rule.

During the audit, we specifically evaluated:

- Alignment of NiSource gas standards (and supporting policies and procedures) with PHMSA Mega Rule requirements
- Processes and controls established to ensure compliance with PHMSA requirements in both execution and documentation activities (pre and post July 1, 2020)
- Management of change activities (including training and communication)

We did not evaluate the completeness of the identified transmission asset population, user access to systems of record, or system back-up and restoration activities.

Internal Audit Finding Ratings

We assign ratings to audit findings based on the following scale (see the Internal Audit Finding Rating Scale in Appendix A):

"1" – Significant Improvement is Needed and Prompt Management Attention is Required

"2" – Improvement is Needed and Management Attention is Necessary

"3" – Some Improvement is Needed and Management Attention is Justified

"4" – Management Evaluation is Desirable

Internal Audit Conclusion and Summary of Observations

The Transmission Integrity Management Program (TIMP) team is actively managing challenges to enable effective and efficient execution of processes that support compliance with the PHMSA Mega Rule. Identifying the complete population of job orders related to transmission pipelines is a key step in establishment of monitoring activities. System programming changes were recently implemented to identify Transmission and Distribution class assets within the work management systems, which will enhance the Company's ability to identify and properly oversee records for transmission assets.

While an assessment has been performed to identify the population of non-TVC transmission assets installed pre-July 1, 2020, minimal progress has been made to address the MAOP and material properties reconfirmation requirements. As the July 2028 deadline approaches to meet the 50 percent completion requirement, we recommend that NiSource management actively work to ensure annual plans incorporate reconfirmation activities (and associated costs) and that appropriate monitoring controls and management reporting are established.

Overall, we found that controls related to compliance with the PHMSA Gas Mega Rule TVC requirements should be improved. We identified one finding associated with inadequate TVC pipeline records which requires management's prompt attention (Rating 1). We also identified one finding where management attention is necessary (Rating 2). In addition, we observed some less-significant items that were discussed with management during the course of the audit.

A summary of audit findings rated "1" through "3" follows (see the Internal Audit Findings Matrix in Appendix B):

- 1) *Traceable, Verifiable and Complete (TVC) Processes and Controls (Post-July 1, 2020)* (Rating 1)
Processes and controls are not sufficient to consistently ensure compliance with PHMSA Mega Rule TVC requirements. Specifically, to ensure that required TVC documentation is captured and retained, as-built drawings should include sufficient detail to correlate drawings with the associated TVC documents, and all documentation is organized and maintained in a manner that facilitates effective and efficient validation and monitoring activities. In addition, training has not been adequate to ensure understanding of roles and responsibilities and quality assurance procedures have not been established to validate and monitor TVC compliance.
- 2) *Quality Assurance Procedures over Third-Party TVC Determination (Pre-July 1, 2020)* (Rating 2)
Oversight of third parties engaged to validate TVC compliance for historical assets (assets installed prior to July 1, 2020) is insufficient to ensure that the TVC compliance conclusions are reliable. Specifically, quality assurance procedures are not formally defined and procedures should address approval and capture of documentation that substantiates complex TVC compliance conclusions (i.e., situations where a combination of records and/or additional explanation is required to substantiate TVC compliance).

Management's Response

Management agrees with the findings noted during this audit and has provided action plans to address the risks identified. Detailed action plans are included in Appendix B. The key mitigation steps will be completed by September 2023.

Internal Audit Follow Up

Management has provided action plans for all findings with a rating of "1", "2", or "3". We have reviewed management's action plans and believe that the action plans will adequately address the findings identified in this audit. We will track the progress of resolution and will conduct follow-up testing for all rated "1" audit findings and a sample of rated "2" and rated "3" audit findings.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Report *****

“1” Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company’s reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

“2” Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

- More than remote probability for damage to the Company’s reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

“3” Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

“4” – Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited



1) <u>Traceable, Verifiable and Complete (TVC) Processes and Controls (Post-July 1, 2020)</u>	<u>Risk Rating: 1</u>
<u>Observation:</u> A mill test report or a certificate of compliance details physical and chemical properties of pipeline materials and includes identifying heat or model numbers for manufactured materials. When utilizing materials provided by external manufacturers, these documents are usually required to meet TVC requirements because they correlate the as-built documentation to the material components that are installed. Processes and controls are insufficient to ensure information required to meet the Pipeline and Hazardous Materials Safety Administration (PHMSA) pipeline transmission TVC requirements is always captured and retained; specifically: • Some roles accountable for various governance, oversight, execution, and support responsibilities that drive adherence to TVC requirements are not clearly identified and comprehensively documented • Some processes are not adequately designed to reliably adhere to TVC requirements; particularly processes to ensure that mill test reports or certificates of compliance are consistently captured and retained, and as-built drawings include sufficient detail to correlate drawings with the associated documents • A standard process has not been established to ensure that information supporting TVC compliance is organized and maintained (within the defined system of record) in a manner that facilitates effective and efficient validation and monitoring activities • Training has been insufficient to ensure that all personnel responsible for aspects of capturing TVC support understand established procedures and their role in TVC compliance • Formal quality assurance procedures to validate and monitor TVC compliance are not established and executed	<u>Management Action Plan:</u> In November 2022, NiSource management performed a “Stand Down” with all impacted groups to discuss the gaps identified in the audit. This included a review of existing documentation, governance and oversight requirements, related gas standards, and roles and responsibilities. Management has engaged with Gas Transmission Systems (GTS), an industry-leading gas utilities and pipeline services expert, to perform a process gap analysis that will include an assessment of defined roles and responsibilities and review of TVC compliance gaps to determine process enhancements and remediation options. The contract with GTS is expected to be finalized by January 2023 and GTS will begin work thereafter. Upon completion of the GTS assessment, management teams will perform the following actions: • Implement remediation plans based on GTS assessment recommendations (TBD - Target remediation date will be dependent on the timing and results of the assessment) • Re-assign TVC LMS training to all impacted parties (January 2023) and ensure adequate course completion (April 2023) • Conduct TVC process training sessions for critical stakeholder groups including Field Engineering, Capital Close-Out, Asset Knowledge Management, Major Projects, and State Construction (April 2023) • Migrate the current TVC database (PODs) to the Utility Pipeline Data Model as part of the OneGIS project scheduled (March 2024) • Utilize Capital Close-Out teams to perform quality control processes to validate TVC compliance (July 2023)

We evaluated compliance with TVC requirements for six work orders completed after July 1, 2020 (the effective date to comply with PHMSA pipeline transmission TVC requirements) and identified that mill test reports or certificates of compliance were not retained or as-built documentation did not adequately reference identifying heat or model numbers for five (of the six) work orders. <u>Criteria:</u> Processes and controls have been established to ensure required TVC documentation is retained, specifically: 1) roles and responsibilities are defined and processes are established to ensure that documents required for TVC compliance are retained; 2) processes and supporting applications are established to retain TVC documentation in a manner that facilitates effective and efficient validation and monitoring activities; 3) impacted field and engineering personnel are adequately trained to ensure process understanding; and 4) quality assurance processes are established to identify exceptions in process execution. <u>Risk:</u> Inadequate pipeline records increase the probability of negative operational outcomes and effective emergency response. Additionally, non-compliance with PHMSA Mega Rule TVC requirements could subject the Company to regulatory fines, penalties, and reputational impact.	- Stand up internal Asset Knowledge Management team that will be responsible for reviewing TVC documentation, performing required field assessments and mapping all recorded and required records within NiSource source of record systems (September 2023) - Utilize the TIMP team to perform quarterly quality control procedures over representative populations of the Asset Knowledge Management team's TVC determinations (September 2023) <u>Responsible:</u> Benjamin Turner, Director Asset Risk Management Aaron Boeke, Director SMS Governance & Execution <u>Resolution Date:</u> See Management Action Plan for key delivery dates.	
2) <u>Quality Assurance Procedures over Third-Party TVC Determination (Pre-July 1, 2020)</u>		<u>Risk Rating:</u> 2
<u>Observation:</u> Oversight of third parties engaged to validate TVC compliance for historical assets (assets installed prior to July 1, 2020) is insufficient to ensure that the TVC compliance conclusions determined by the third parties are reliable; specifically: Some statements of work for third-party contractors performing TVC determinations do not specify that TVC determinations must be made in accordance with NiSource gas standards, policies, and procedures	<u>Management Action Plan:</u> Management teams will perform the following actions: - Utilize GTS to assess potential gaps associated with TVC compliance for the pre-July 1, 2020 asset population (TBD) - Develop and implement processes to require leadership review of contracts for services performed by third parties, including approval of contract terms, scopes of work and requirements. (February 2023) - Utilize the Asset Knowledge Management team to perform quality assurance reviews over third-party TVC determinations and	

- Quality assurance procedures are not formally defined and executed to monitor the accuracy and reliability of TVC compliance conclusions determined by third parties
- Procedures are not formally established to approve and capture documentation that substantiates complex TVC compliance conclusions (i.e., situations where a combination of records and/or additional explanation is required to substantiate TVC compliance) made by third parties

We evaluated sample job orders to verify the TVC compliance conclusions determined by third parties and identified that some transmission pipeline asset features determined to be TVC compliant by a third party were not supported by documentation that was sufficient to comply with TVC requirements. Also, processes to document complex TVC compliance conclusions were not executed per the NiSource gas standards requirements.

Criteria:

Processes to oversee and monitor third parties engaged to validate TVC compliance for historical assets are sufficient to ensure that TVC compliance conclusions are reliable; specifically: 1) statement of work terms are robust and clearly define the scope of work and relevant parameters; 2) procedures to validate that third party TVC compliance conclusions are reliable are defined and executed; and 3) procedures to approve and document information to substantiate complex TVC compliance conclusions are established and executed per NiSource gas standards requirements.

Risk:

Reliance on third-party TVC determinations may negatively impact NiSource's ability to accurately identify and adequately manage the population of non-TVC transmission assets subject to future maximum allowable operating pressure reconfirmation requirements. Additionally, non-compliance with PHMSA Mega Rule TVC requirements could subject the company to significant regulatory fines and penalties.

adherence to NiSource procedures and TVC documentation requirements (July 2023)

Responsible:

Benjamin Turner, Director Asset Risk Management
Aaron Boeke, Director SMS Governance & Execution

Resolution Date:

See Management Action Plan above for key delivery dates.

NiSource, Inc.

Treasury Operations General Controls

Internal Audit Report

Distribution

Respondents

Randy Hulen
Kristen King

Beneficiaries

Gunnar Gode

For Information

Shawn Anderson
Melanie Berman
Melody Birmingham
Donald Brown
Kimberly Cuccia
William Jefferson
Lloyd Yates

Internal Audit Report

Background

The Treasury department supports the cash management activities for NiSource, Inc. (NiSource or “the Company”) and its subsidiaries (Northern Indiana Public Service Company, the Columbia Gas Distribution Companies and all joint ventures). During 2021 and the nine months ended September 30, 2022, the department executed \$15.5 billion and \$15.0 billion, respectively, in payments, while managing \$9.2 billion and \$9.5 billion, respectively, in long term debt. The Company also maintains a \$1.85 billion revolving credit facility.

Audit Objective, Approach, and Coverage

The objective of this risk-based internal audit was to provide an independent evaluation of the adequacy, effectiveness, and efficiency of controls associated within Treasury operations. At the beginning of our audit, we completed a risk assessment, and we conducted detailed process assessments and sample-based transactional testing in higher-risk areas. The review period for this audit was October 1, 2021 through September 30, 2022.

During the audit, we specifically evaluated processes and controls related to:

- Financial strategy, including short-term and long-term strategic cash management, cash/liquidity forecasting, interest rate swaps, and debt covenant compliance
- Approval of debt and equity transactions
- Regulatory risk management activities associated with intercompany borrowing requirements
- System interface, access, and segregation of duties considerations for the GTreasury application
- Associated accounting, including debt and interest payment and disbursement activities and account reconciliations

We did not evaluate bank account approval and creation processes due to low transaction volume.

Internal Audit Finding Ratings

We assign ratings to audit findings based on the following scale (see the Internal Audit Finding Rating Scale in Appendix A):

“1” – Significant Improvement is Needed and Prompt Management Attention is Required

“2” – Improvement is Needed and Management Attention is Necessary

“3” – Some Improvement is Needed and Management Attention is Justified

“4” – Management Evaluation is Desirable

Internal Audit Conclusion and Summary of Observations

The Treasury department has a well-defined and structured strategy and processes for managing the Company’s short-term and long-term capital needs. However, we observed that the current Sarbanes-Oxley (SOX) control framework can be enhanced to address all key control elements and risks associated with Treasury operations and is currently reliant upon the account reconciliation control to catch material misstatements in the cash and debt account balances. We recommend that management revisit the SOX risk and control environment to ensure controls have been identified and formalized to address key risks and to alleviate stress on the account reconciliation control.

Overall, we found that processes and controls related to Treasury operations (as specified in the “Audit Objective, Approach, and Coverage” section of this report) were generally operating as intended. We did, however, identify one finding where management’s attention is justified (Rating 3). In addition, we observed some less significant items that were discussed with management during the audit.

A summary of audit findings rated “1” through “3” follows (see the Internal Audit Findings Matrix in Appendix B):

1) Treasury Operation Risk and Controls Framework (Rating 3)

The current SOX control framework and scope of testing performed should be enhanced to ensure the completeness and accuracy of cash and debt account balances within the Company’s financial statements.

Management’s Response

Management agrees with the finding noted during this audit and has provided action plans to address the risks identified. Detailed action plans are included in Appendix B. The key mitigation steps will be completed by September 2023.

Internal Audit Follow Up

Management has provided action plans for all findings with a rating of “1”, “2”, or “3”. We have reviewed management’s action plans and believe that the action plans will adequately address the findings identified in this audit. We will track the progress of resolution and will conduct follow-up testing for all rated “1” audit findings and a sample of rated “2” and rated “3” audit findings.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Report *****

“1” Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company’s reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

“2” Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

- More than remote probability for damage to the Company’s reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

“3” Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

“4” Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited



1) <u>Treasury Operations Risk and Controls Framework</u>	<u>Risk Rating: 3</u>
<u>Observation:</u> The Sarbanes-Oxley (SOX) Compliance team and the Treasury department are responsible for identifying risks and controls to ensure cash and debt account balances are recorded completely and accurately in the financial statements. These controls are subject to annual testing by the SOX Compliance team. The current SOX control framework and scope of testing should be enhanced; specifically: • A control to validate the completeness and accuracy of transactions transmitted from the GTreasury system to PeopleSoft and resolve identified exceptions is not performed or included in the SOX framework • The documented control procedures for two SOX reconciliation controls (daily short-term pool of funds activity worksheet and the swap reasonableness review) do not include a formalized and evidenced review step and review/approval of these reconciliations is not evidenced; as a result, we were unable to validate that these reconciliations were appropriately reviewed • The monthly confirmation statement reconciliation is currently performed, reviewed/approved and evidenced for short-term debt; however, the review/approval of this control has not been formalized within the existing SOX control and has not been included as a step within the SOX testing. Additionally, the control does not include a formalized and evidenced review step for the long-term debt balance and as a result, we were unable to validate that the long-term debt reconciliation was appropriately reviewed <u>Criteria:</u> Processes and controls are sufficient to ensure that SOX controls are properly identified, executed, and tested to address the risk of incomplete and/or inaccurate cash and debt balances within the financial statements; specifically: 1) risks and controls are formally identified and codified within the SOX control framework; 2) controls are	<u>Management Action Plan:</u> Treasury management has completed the following actions: • Formalized a process to obtain and review the daily data transfer email notification to ensure all transactions were transmitted completely and accurately from GTreasury into PeopleSoft, including exception investigation and resolution • Formalized a process to document and retain evidence of review of the short-term pool of funds activity worksheet • Formalized a process to document and retain evidence of review of the swap reasonableness review • Formalized a process to document and retain evidence of review for the monthly confirmation statement reconciliation for long-term debt SOX Compliance management will complete the following actions: • Formalize the review of the data transmission between GTreasury and PeopleSoft within the SOX control framework • Formalize the review of the short-term pool of funds activity worksheet within the existing SOX control and update control testing procedures accordingly • Formalize the review of the swap reasonableness review within the existing SOX control and update control testing procedures accordingly • Formalize the review of the monthly confirmation statement reconciliation for both short-term and long-term debt balances within the existing SOX control and update control testing procedures accordingly

timely executed and evidenced; 3) controls are tested; and 4) testing is properly documented, including formal sign-off by the process owner and a SOX Compliance team member in the SOX data management application.

Risk:

Potential that cash account misstatements are not timely identified and resolved leading to a financial reporting misstatement; also, potential that daily cash funding needs are not accurately identified, resulting in an inability to fund operations.

Responsible:

Randy Hulen, VP Investor Relations and Treasury
Kristen King, Director Consolidations, External Reporting, Technical Accounting, & SOX

Resolution Date:

Treasury management has formalized and implemented the processes outlined above related to the review of the daily data transfer email notification, the short-term pool of funds activity worksheet, the swap reasonableness review, and the monthly confirmation statement reconciliation for long-term debt.

The SOX Compliance team will partner with the Treasury management team to complete the action steps noted above by September 2023, including testing the operating effectiveness of the enhanced formalized processes.

***** End of Report*****

NiSource Corporate Services Company

Gas Supply General Controls

Internal Audit Report

Distribution

Respondents

Brad Stuck
Adam Gale

Beneficiaries

Karl Stanley
Scott Diener

Other Key Personnel

Andy Campbell Gunnar Gode Kristen King
Patrick Pluard

For Information

Shawn Anderson
Melanie Berman
Melody Birmingham
Donald Brown
Kimberly Cuccia
William Jefferson
Lloyd Yates

Internal Audit Report

Background

The NiSource Energy Supply & Optimization (ES&O) team manages gas supply for nearly four million NiSource Inc. (NiSource or “the Company”) customers located in six states. The team is responsible for natural gas procurement processes and facilitating activities to move the physical gas across the system and into/out of storage for all six NiSource Local Distribution Companies (LDCs). The ES&O team procured 215 MMDth of natural gas at a cost of \$793.6 million in 2021 and 167 MMDth at a cost of \$1.1 billion through the third quarter of 2022. The year over year increase in expense was a result of the dramatic increase in the commodity price of natural gas during 2022.

The ES&O, Demand Forecast, and Gas Control teams perform forecasts for each LDC daily, monthly, and seasonally in consideration of multiple factors, including customer demand, weather, and storage capacities. The forecasts drive gas supply planning processes and procurement decisions. The teams use various applications to manage gas planning and forecasting (NiEMS and EASy), as well as trading (GasSource) activities, and important controls are automated within these applications.

Audit Objective, Approach, and Coverage

The objective of this risk-based internal audit was to provide an independent evaluation of the adequacy, effectiveness, and efficiency of controls associated with gas supply activities. At the beginning of our audit, we completed a risk assessment, and we conducted detailed process assessments and sample-based transactional testing in higher-risk areas. The review period for this audit was June 2021 through June 2022.

During the audit, we specifically evaluated processes and control related to:

- Forecasting, including model selection, change management review and approval processes, and monitoring of forecasted versus actual results
- Procurement activities, including supplier approval, nominating, and scheduling activities, and invoice review and approval
- System access and segregation of duties considerations for gas supply planning, forecasting, and trading systems
- Completeness and accuracy of gas supply information provided to the Regulatory team
- The adequacy of policies and procedures for gas supply-related activities
- Completeness and accuracy of gas supply information provided to the Accounting team

We did not evaluate processes and controls related to off-system sales (including park and loan activity) due to lower materiality and hedging due to a limited volume of activity.

Internal Audit Finding Ratings

We assign ratings to audit findings based on the following scale (see the Internal Audit Finding Rating Scale in Appendix A):

“1” – Significant Improvement is Needed and Prompt Management Attention is Required

“2” – Improvement is Needed and Management Attention is Necessary

“3” – Some Improvement is Needed and Management Attention is Justified

“4” – Management Evaluation is Desirable

Internal Audit Conclusion and Summary of Observations

While the NiSource Energy Supply & Optimization team is focused on continuous improvement, we noted that the effectiveness of some key activities, including forecasting and system access reviews, are heavily reliant upon the knowledge and expertise of the employees performing the tasks as opposed to a reliable control framework. We recommend that management formalize oversight and monitoring controls in these areas to ensure consistency and facilitate knowledge transfer.

We found that processes and controls related to the gas supply general controls (as specified in the "Audit Objective, Approach, and Coverage" section of this report) were generally operating as intended. We did, however, identify two findings where management's attention is justified (Rating 3). In addition, we observed some less-significant items that were discussed with management during the audit.

A summary of audit findings rated "1" through "3" follows (see the Internal Audit Findings Matrix in Appendix B):

- 1) *Gas Planning, Forecasting, & Trading System Access Review Controls* (Rating 3)
User access is periodically reviewed for the gas planning, forecasting, and trading systems; however, the system access roles configured within these technology solutions are not formally defined and documented and the effectiveness of access reviews is reliant upon reviewers' understanding and knowledge of system roles.
- 2) *Gas Supply Forecast Review & Approval Controls* (Rating 3)
Formal review and approval of forecasts and associated documentation are not required per current policies and procedures and as a result, we were unable to validate that the review and approval activities for the monthly and seasonal forecasts occur consistently.

Management's Response

Management agrees with the findings noted during this audit and has provided action plans to address the risks identified. Detailed action plans are included in Appendix B. The key mitigation steps will be completed by September 2023.

Internal Audit Follow Up

Management has provided action plans for all findings with a rating of "1", "2", or "3". We have reviewed management's action plans and believe that the action plans will adequately address the findings identified in this audit. We will track the progress of resolution and will conduct follow-up testing for all rated "1" audit findings and a sample of rated "2" and rated "3" audit findings.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Report *****

“1” Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company’s reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

“2” Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

- More than remote probability for damage to the Company’s reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

“3” Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

“4” – Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited



1) <u>Gas Planning, Forecasting, & Trading System Access Review Controls</u>	<u>Risk Rating: 3</u>
<u>Observation:</u> Multiple processes are automated within various technology applications used by the Energy Supply & Optimization (ES&O) team, and appropriate system access is imperative to maintaining segregation of duties and ensuring that users' access to system functionality is consistent with their job responsibilities. While the ES&O team reviews users' access for the GasSource, EASy and NiEMS systems, the system access roles configured within these technology solutions are not formally defined and documented. Therefore, the effectiveness of access reviews is reliant upon reviewers' understanding and knowledge of system roles, which could impair the reliability and consistency of these activities. We worked with the Information Technology organization to understand the role definitions for each system and reperformed the access review. We found system access to be consistent with users' job responsibilities and did not identify any segregation of duties risks. <u>Criteria:</u> Controls and processes are sufficient to ensure that system access is appropriate based on assigned roles and responsibilities and segregation of duties is maintained; specifically: 1) system access assignments are formally reviewed against system role definitions to ensure they are appropriate based upon job function and consistent with assigned responsibilities; 2) appropriate segregation of duties is maintained; 3) new access or changes to access levels has been approved by the system administrator; and 4) user additions and deletions are processed in a timely manner. <u>Risk:</u> System access is not adequately restricted resulting in inappropriate segregation of duties and/or lack of data integrity.	<u>Management Action Plan:</u> ES&O management will perform the following actions: • Develop and maintain a listing of system role definitions for the GasSource, EASy, and NiEMS systems that define the specific access and permission levels granted for each role • Utilize the system role definitions listing during the semi-annual system access review process to ensure user access is appropriate <u>Responsible:</u> Brad Stuck, Director Supply Development <u>Resolution Date:</u> September 2023

2) <u>Gas Supply Forecast Review & Approval Controls</u>	<u>Risk Rating: 3</u>
<u>Observation:</u> The ES&O, Demand Forecast, and Gas Control groups prepare daily, monthly, and seasonal (also referred to as design day) forecasts to identify gas supply needs based upon weather, storage, and customer demand. These forecasting activities are the foundation for all other gas supply activities. While informal management review and approval processes occur, formal review and approval of forecasts and associated documentation are not required per current policies and procedures. As a result, we were unable to validate that the review and approval activities for the monthly and seasonal forecasts occur consistently. <u>Criteria:</u> Controls and processes are sufficient to ensure that gas supply forecasting is sufficient to meet daily customer demand; specifically: 1) processes to prepare and timely review periodic gas supply forecasts are formalized; 2) access to make changes to the forecasting models is restricted based upon roles and responsibilities; 3) processes are formalized to review and approve changes to the forecasting models; and 4) processes are formalized to compare forecasts to actual results against a predetermined threshold to determine if changes to the forecast or model selection determination are necessary. Variances over the threshold not requiring changes are explained and documented. <u>Risk:</u> Potential that insufficient forecasting activities lead to a shortage of gas supply and storage impacting the ability to meet customer demand, resulting in a financial loss and negative reputational impact with customers and regulators.	<u>Management Action Plan:</u> Demand Forecast management will perform the following actions: • Formalize monthly (for NIPSCO and Columbia Gas Local Distribution Companies (LDC)) and seasonal forecast (for NIPSCO) review and approval processes and modify policies and procedures to require these activities be performed and evidenced • Maintain evidence of reviewed monthly and seasonal forecasts within a centralized location for a time period consistent with the Company's records retention policy Energy Supply & Optimization management will perform the following actions: • Formalize design day forecast (for LDCs) review and approval processes and modify policies and procedures to require these activities be performed and evidenced • Maintain evidence of reviewed design day forecasts within a centralized location for a time period consistent with the Company's records retention policy <u>Responsible:</u> Adam Gale, Director Demand Forecasting Brad Stuck, Director Supply Development <u>Resolution Date:</u> June 2023
3) <u>Gas Usage Variance Analysis Controls</u>	<u>Risk Rating: 4</u>
<u>Observation:</u> The Gas Planning & Forecasting team utilizes the daily Mean Absolute Percentage Error (MAPE) rate review to compare actual versus forecasted weather and gas usage to determine whether a change to	A management response is not requested; however, Internal Audit recommends that management:

the forecast or model selected and utilized to meet gas supply demand is justified. Currently, a defined threshold against which to evaluate MAPE rate variances has not been formalized for each of the LDCs. While the gas supply forecasts were generally accurate for the period under review, with significant deviations between forecasts and actual gas used occurring for only short durations of time, evaluating variances against defined thresholds would provide the opportunity to drive reliability and consistency in the forecasting process, while facilitating potential forecast and model refinement and providing support for decision making.

Criteria:

Controls and processes are sufficient to ensure that gas supply forecasting is sufficient to meet daily customer demand; specifically: 1) processes to prepare and timely review periodic gas supply forecasts are formalized; 2) access to make changes to the forecasting models is restricted based upon roles and responsibilities; 3) processes are formalized to review and approve changes to the forecasting models; and 4) processes are formalized to compare forecasts to actual results against a predetermined threshold to determine if changes to the forecast or model selection determination are necessary. Variances over the threshold not requiring changes are explained and documented.

Risk:

Potential that insufficient forecasting activities may lead to a shortage of gas supply impacting the ability to meet customer demand, resulting in a financial loss and negative reputational impact with customers and regulators.

- Define and utilize a formalized threshold for each of the Columbia LDCs (or at a more granular level as appropriate) against which to evaluate MAPE rate variances to determine if changes to the forecast or model selection are appropriate
- Document analysis performed, including whether forecast or model changes should be considered for identified variances over the threshold

***** End of Report*****

NiSource Inc.

Customer Credit and Collections Processes

Internal Audit Report

Distribution

Respondents

Bryan Adams

Venkatesh Iyer
Angela Sanchez

Laura Rosenthal

Beneficiaries

Waco Bankston
Kevin Johannsen

Michele Caddell
Jennifer Montague
Kevin Stanley

Gunnar Gode
Charles Shafer

For Information

Shawn Anderson
Melanie Berman
Melody Birmingham
Donald Brown
Kim Cuccia
William Jefferson
Lloyd Yates

Internal Audit Report

Background

NiSource Inc. (NiSource or the Company) serves approximately 3.6 million gas and 470,000 electric customers across six states. The Meter to Cash department is responsible for revenue recovery and field collection activities and utilizes a combination of company and third-party resources. Some collections activities, such as termination notices, are automated within the applicable customer billing systems while other activities, including field collections and shut off orders, must be manually executed. As of December 2022, NiSource customer arrearages totaled \$120.9 million.

Audit Objective, Approach, and Coverage

The objective of this risk-based internal audit was to provide an independent evaluation of the adequacy, effectiveness, and efficiency of controls associated with customer credit and collections processes. At the beginning of our audit, we completed a risk assessment, and we conducted detailed process assessments and sample-based transactional testing in higher-risk areas. The review period for this audit was January 2020 through May 2022.

During the audit, we specifically evaluated:

- Compliance with pandemic-related moratoriums issued by state regulatory commissions for requirements in effect during the audit period
- Accuracy of pandemic-related accounting entries, including the associated bad debt regulatory asset
- Adherence to regulatory or company policies related to customer termination notices, termination of service activities, customer bankruptcies, and winter moratoriums
- Outreach activities to customers in arrears
- Adjustments to employees' personal utility accounts

We did not evaluate qualification and acceptance processes related to state-specific payment plans and programs, processes to maintain accuracy of customer contact information, or post write-off processes, and these areas will be considered for review in future audits.

Internal Audit Finding Ratings

We assign ratings to audit findings based on the following scale (see the Internal Audit Finding Rating Scale in Appendix A):

"1" – Significant Improvement is Needed and Prompt Management Attention is Required

"2" – Improvement is Needed and Management Attention is Necessary

"3" – Some Improvement is Needed and Management Attention is Justified

"4" – Management Evaluation is Desirable

Internal Audit Conclusion and Summary of Observations

The Meter to Cash team successfully navigated unprecedented circumstances resulting from pandemic-related moratoriums and rapidly changing collections requirements, which required significant coordination and alignment with various key stakeholders across the Company. As the pandemic drove up arrearage balances and the recent economic downturn is placing strain on customers' ability to pay, the team recently initiated a customer

engagement strategy to increase proactive and targeted communications to customers at risk of falling into arrears. As this program matures, we recommend continued monitoring of its impact and consider any need for refinement.

We found that processes and controls associated with collections activities were generally operating as intended. We did, however, identify two findings where management's attention is necessary (Rating 2) and two findings where management's attention is justified (Rating 3). In addition, we observed some less-significant items that were discussed with management during the course of the audit.

A summary of audit findings rated "1" through "3" follows (see the Internal Audit Findings Matrix in Appendix B):

- 1) Compliance Related to Termination-of-Service Notification Requirements (Rating 2)
A programming logic error within the DIS customer billing system is resulting in some termination-of-service job orders being generated within a timeframe that does not comply with tariff requirements.
- 2) Vendor Governance Related to Field Collection Activities (Rating 2)
Processes are not adequate to identify vendors with unacceptable performance against measured safety metrics and timely develop and implement appropriate risk mitigation steps.
- 3) NIPSCO Retention of Documents for Customer Bankruptcy Cases (Rating 3)
Procedures have not been developed to ensure that document retention policy requirements specific to NIPSCO customer bankruptcies are followed, and documents are not retained per the policy requirements.
- 4) Monitoring of Employee Accounts (Rating 3)
The current customer account management and billing systems used by NiSource do not include a data field enabling employee accounts to be efficiently tracked and monitored. While manual procedures have been established to track and monitor adjustments to employee accounts associated with the Columbia Gas Companies, similar procedures have not been established to review NIPSCO employee accounts.

Management's Response

Management agrees with the findings noted during this audit and has provided action plans to address the risks identified. Detailed action plans are included in Appendix B. The key mitigation steps will be completed by December 2023.

Internal Audit Follow Up

Management has provided action plans for all findings with a rating of "1", "2", or "3". We have reviewed management's action plans and believe that the action plans will adequately address the findings identified in this audit. We will track the progress of resolution and will conduct follow-up testing for all rated "1" audit findings and a sample of rated "2" and rated "3" audit findings.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Report *****

“1” Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company’s reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

“2” Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

- More than remote probability for damage to the Company’s reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

“3” Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

“4” – Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited



1) <u>Distributive Information System (DIS) Program Logic Error Resulting in Termination of Service Executed with Insufficient Notice to Columbia Gas Customers</u>	<u>Risk Rating: 2</u>
<u>Observation:</u> The primary control to ensure that the timeframe between when a customer is notified that service will be terminated due to non-payment and when the service termination job order is in line with tariff requirements is automated within the Columbia Gas Companies' Distributive Information System (DIS) program logic. Historical DIS program change management controls were not adequate to prevent a programming logic error that is resulting in some termination of service job orders being generated within a timeframe that does not comply with tariff requirements. We analyzed termination of service transactions between January 2021 and July 2022 and identified some instances where the timeframe between system-generated customer notifications and termination of service job orders were not in line with tariff requirements. <u>Criteria:</u> System application change management controls are sufficient to ensure that program changes operate per business requirements, specifically: 1) change management procedures are formalized; 2) program changes are processed in a development environment and tested in a frozen test environment; 3) the duties of programming, testing, and promoting changes to production are appropriately segregated/controlled; and 4) changes are sufficiently tested (unit and functional) using appropriate test scripts and formally accepted by the business owner prior to being promoted to the production environment. <u>Risk:</u> Potential for noncompliance with tariff requirements leading to customer complaints, potential regulatory enforcement, and reputational damage.	<u>Management Action Plan:</u> The IT Applications team notes that the functionality in the DIS collections processing has been in place for quite some time (well over a decade) and there have been no recent programming changes in this functional area. Although there may have been an issue in the historical change management process for this functionality, management is confident in the effectiveness of the current robust change management process. Until the historic logic errors can be identified and remediated, IT Applications management has taken the following action (this process will remain in place until a permanent fix is implemented): • Implement a monitoring process utilizing a query generated daily to identify and delete shut-off orders that are scheduled outside of the normal collections window Additionally, IT Applications will take the following actions which will replace the daily query process upon implementation: • Add additional logic in DIS collections to prevent processing shut-off orders for accounts that are outside of the collections window • Execute change management activities to ensure logic changes are operating as intended <u>Responsible:</u> Venkatesh Iyer, Director IT Applications <u>Resolution Date:</u> Additional programming logic will be implemented by February 2023.

2) Vendor Governance Related to Field Collection Activities

Risk Rating: 2

Observation:

The Credit and Collections team engages third-party vendors to conduct field collection activities on behalf of NiSource, and NiSource uses the ISN Software Corporation ISNetworld platform (ISNetworld) to monitor safety and other important performance metrics for vendors. Processes to identify vendors with unacceptable performance against measured ISNetworld metrics and timely develop and implement appropriate risk mitigation steps are not adequate; specifically:

- Statements of work for third-party vendors performing field collections activities require the contractors to subscribe to the ISNetworld service but do not specify penalties or the potential for contract termination if the vendor receives a failing grade and is unable to implement mitigation steps
- Procedures to review field collection vendors' performance against the ISNetworld measured metrics are not formalized and monitored
- Processes to formally evaluate potential risk to NiSource related to field collection vendors with unacceptable ratings are not timely performed and potential risk is not actively monitored and managed and/or appropriate exception processes are not timely completed
- Performance improvement plans are not developed and monitored for vendors with substandard ratings

At the time of our review, two of the three vendors executing field collections activities had unacceptable ratings in ISNetworld; however, the required exception process (a variance letter submitted by the vendor and approved by the NiSource Chief Safety Officer) was not timely executed.

Criteria:

Policies and procedures are adequately designed and executed to ensure third-party contractors performing work on behalf of the Company meet safety and performance standards, specifically: 1)

Management Action Plan:

Meter to Cash management will incorporate monitoring of the ISNetworld metrics into the current business review process conducted for the first quarter of 2023 (April 2023).

Additionally, as all contracts for field collections work expire in September 2023, Meter to Cash management will begin the request for proposal process in January 2023 and plan to incorporate the action plans below:

- Update contract language for newly contracted field collections vendors to specify clear expectations for the ISNetworld process and consequences for failing to meet expectations (August 2023)
- Identify contingencies if operations are disrupted because a vendor with unacceptable safety performance fails to receive a variance (August 2023)

The Safety Services team will perform the following actions:

- Grant ISNetworld access to Meter to Cash team leaders and managers (February 2023)
- Provide ISNetworld user training to Meter to Cash team leaders and managers (March 2023)

Responsible:

Laura Rosenthal, Director Meter Reading and Revenue Recovery
Bryan Adams, Director Safety Services and Occupational Safety

Resolution Date:

Refer to action plan dates above.

contract terms specifically define measured metrics and potential outcomes of penalties for inadequate performance, 2) roles and responsibilities related to contractor governance are clearly defined, 3) results of contractor assessments are reviewed timely to determine if additional action is required, 4) submissions for variances are reviewed and approved timely, 5) contractors who do not meet safety and performance standards and who do not have an active variance are prevented from performing work on the Company's behalf until required remediations are completed. <u>Risk:</u> Potential that a vendor's unacceptable performance against measured safety and other performance metrics presents safety or operational risk to NiSource.	
3) <u>Northern Indiana Public Service Company (NIPSCO) Retention of Documents for Customer Bankruptcy Cases</u>	<u>Risk Rating:</u> 3
<u>Observation:</u> The NIPSCO policy outlining requirements for processing customer bankruptcies, which was last reviewed and approved in 2019, explicitly specifies that certain documents should be retained as Company records. Procedures to ensure that document retention policy requirements are adhered have not been developed, and documents are not retained per the policy requirements. <u>Criteria:</u> Company policies clearly define roles, responsibilities, and process requirements and support the achievement of business objectives and risk management strategies. <u>Risk:</u> Potential that Company policies are misaligned with business risk and objectives and/or not adhered to, which could expose NiSource to regulatory and legal risk or could result in company resources being diverted to lower risk activities.	<u>Management Action Plan:</u> Revenue Recovery will update NIPSCO policies associated with customer bankruptcies to align with state and federal requirements and current business practices. Policies will be reviewed to identify opportunity for alignment with other operating companies where applicable. Once policies are updated, the Revenue Recovery team will be given training on updated policies and documented processes. <u>Responsible:</u> Laura Rosenthal, Director Meter Reading and Revenue Recovery <u>Resolution Date:</u> December 2023

4) <u>Monitoring of Employee Accounts</u>	<u>Risk Rating: 3</u>
<u>Observation:</u> Identifying the complete population of customer accounts related to NiSource employees is a key step in establishing efficient and effective monitoring activities to ensure employees who have access in the billing systems to adjust customer accounts do not make inappropriate adjustments to their own accounts or to the accounts of other employees. The current customer account management and billing systems used by NiSource do not include a data field enabling employee accounts to be efficiently tracked and monitored. Also, while manual procedures have been established to track and monitor adjustments to employee accounts associated with the Columbia Gas Companies, similar procedures have not been established to review all NIPSCO accounts. We analyzed adjustments to employee accounts and did not identify indications of inappropriate adjustments. <u>Criteria:</u> Controls and processes are sufficient to ensure that employees do not improperly utilize customer billing system access on personal accounts or the accounts of other employees, specifically: 1) a complete population of employee accounts is either manually tracked or systemically identified; 2) employees with access to perform higher-risk functions within the customer information and billing systems are identified; 3) controls are established and executed to monitor higher risk activities on employee accounts and identified exceptions are investigated and resolved. <u>Risk:</u> Potential for inappropriate adjustments by employees on their own personal accounts or other employees' accounts are not identified or remediated.	<u>Management Action Plan:</u> Management will consider whether system enhancements would be possible to include a data field within the customer billing systems identifying employee accounts. Additionally, management will establish manual review procedures (similar to those executed for the Columbia Gas Companies) to identify NIPSCO employee accounts and implement monitoring procedures to ensure NIPSCO employees do not inappropriately adjust their own or other employees' accounts. <u>Responsible:</u> Angela Sanchez, Director Gas Transportation Program and Customer and Industrial Billing <u>Resolution Date:</u> December 2023
5) <u>Human Error Resulting in Termination of Service Executed with Insufficient Notice to Columbia Gas Customers</u>	<u>Risk Rating: 4</u>
<u>Observation:</u> We analyzed termination of service transactions between January 2021 and July 2022 and identified seven instances where the timeframe between the customer notifications and termination of service was not	A management action plan is not requested for this finding, but Internal Audit recommends that management enhance training and monitoring activities related to the collections processes where compliance exceptions were identified, specifically:

in line with tariff requirements due to field technicians improperly terminating service when completing collections job orders and three instances due to Revenue Recovery personnel incorrectly creating manual shutoff job orders. Criteria: Controls are sufficient to ensure that customer notices are issued in accordance with regulatory requirements prior to termination of service for non-payment; specifically: 1) personnel responsible for creating or executing collections job orders are adequately trained and understand compliance requirements, and 2) higher risk transactions are independently verified before being processed/executed. Risk: Non-compliance with customer notification requirements may result in customer complaints, potential regulatory enforcement, and reputational damage.	• Hold refresher training to reinforce processes and requirements for all CPA service technicians responsible for executing collections job orders and consider establishing monitoring processes to create feedback loops and verify adherence after the training • Reinforce notice timeframe requirements with Revenue Recovery personnel and consider establishing monitoring processes to create feedback loops and verify adherence after the training • Consider implementing a secondary review/validation control related to manual shutoff job orders
6) <u>Revenue Recovery Outreach Activities for Columbia Gas Transportation Service Customers</u>	<u>Risk Rating: 4</u>
Observation: To encourage customers participating in the Columbia Gas Companies gas transportation service (GTS) program to adhere to their contract terms and remain current on outstanding balances, the NiSource Revenue Recovery team formally reviews customer balances monthly and contacts customers with arrears balances. Outreach activities and any subsequent actions taken on customers' accounts are manually tracked in a spreadsheet maintained by a Revenue Recovery Specialist; however, completion of tracked activities is not verified. During one month in 2022 following personnel transition, outreach did not occur for some GTS customers with arrears. Criteria: Collections activities are consistently executed and evidenced, and management review controls are adequate to ensure execution deficiencies are identified and remediated timely.	A management action plan is not requested for this finding, but Internal Audit recommends that management consider incorporating a second level review and sign-off of the GTS outreach tracking spreadsheet to ensure outreach activities occurred as expected.

<u>Risk:</u> Potential that inconsistently executed control activities negatively impact operational results.	

***** End of Report*****



Internal Audit Department



We exist to deliver safe, reliable energy that drives value to our customers

Geographic Information System (GIS) – Information Technology (IT) General Controls

Internal Audit Report

Distribution

Respondents:

Aaron Boeke
Diego Castillo
Jeremy Plante
Ishreth Sameem

Beneficiaries:

Waco Bankston
Percell Berry
Carla Donev
Robert Kandell
William Mojica
Gregory Skinner

For Information:

Shawn Anderson
Melanie Berman
Melody Birmingham
Donald Brown
Kim Cuccia
William Jefferson
Lloyd Yates



Internal Audit Report

Background

NiSource Inc. (NiSource or the Company) utilizes GIS to manage, analyze, and display geographic information, including information on current pipeline infrastructure, and GIS is the system of record for gas pipeline asset locations. NiSource's GIS platform consists of 32 applications and six databases (one database for Northern Indiana Public Service Company, which includes both gas and electric, and databases for each of the Columbia Gas Distribution Companies).

Approximately 5,400 users have access to GIS, and 250.5 million records are maintained within the system. Field personnel access mapping data through the Field Maps application on their mobile devices or through offline copies of GIS data digital versatile disc (DVD) or universal serial bus (USB) drives. Users with update access to GIS data primarily access GIS through a Citrix virtual session.

Audit Objective, Approach, and Coverage

The objective of this risk-based internal audit was to provide an independent evaluation of the adequacy, effectiveness and efficiency of controls associated with the GIS platform. We completed a risk assessment and conducted detailed process assessments and sample-based transactional testing in higher risk areas. The review period associated with the GIS transactions evaluated during this audit was October 2021 through September 2022.

During the audit, we specifically evaluated processes and controls related to:

- Access and password management
- Disaster recovery and business continuity
- Change management (including application changes and technology changes)
- Data integrity and security management
- Technology configurations and program change security review processes

We did not evaluate project controls and third-party vendor management related to the GIS enhancements implementation project. Additionally, we did not evaluate patch management as this process will be subject to a separate audit scheduled to be performed during 2023.

Internal Audit Finding Ratings

Internal Audit assigns ratings to audit findings based on the following scale (see the Internal Audit Finding Rating Scale in Appendix A):

“1” – Significant Improvement is Needed and Prompt Management Attention is Required

“2” – Improvement is Needed and Management Attention is Necessary

“3” – Some Improvement is Needed and Management Attention is Justified

“4” – Management Evaluation is Desirable

Internal Audit Conclusion and Summary of Observations

The GIS Applications team is focused on enhancing access to current mapping information, including the implementation of OneGIS and Lemur, which will improve offline mapping capabilities. Multiple business and technology teams are involved in ensuring the accuracy of GIS data and reliability of GIS functionality, and these various teams tend to operate in silos that do not always effectively communicate, which could lead to misalignment regarding risk management prioritization. We recommend formalizing a GIS application support council (including the GIS Applications, Asset Knowledge Management, Cybersecurity, and Innovation Compliance and Risk teams) that meets periodically to discuss risk and vulnerabilities and align on risk mitigation prioritization.

Overall, we found that processes and controls related to the GIS application (as specified in the “Audit Objective, Approach, and Coverage section of this report) should be improved. We identified two findings requiring management’s

prompt attention (Rating 1) related to monitoring technology risks and vulnerabilities associated with the GIS application and compliance with password policy requirements. We also identified two findings where management's attention is necessary (Rating 2). In addition, we observed some less-significant items that were discussed with management during the audit.

A summary of audit findings rated "1" through "3" follows (see the Internal Audit Findings Matrix in Appendix B):

- 1) GIS Application Risk and Vulnerability Analysis (Rating 1)
Processes to evaluate risks and vulnerabilities are not formalized for some applications, including the GIS application. Some risks and vulnerabilities associated with GIS were not being reviewed on a regular basis by the GIS Applications, Asset Knowledge Management, Cybersecurity, or Innovation Compliance and Risk teams. As a result, risks and vulnerabilities related to the GIS application may not be adequately evaluated and actioned. Over 1,000 risks/vulnerabilities identified during Qualys scans had not been formally assessed by the Cybersecurity, GIS Applications, or the Innovation Compliance and Risk teams and discussed with the GIS application owners from a potential-for-business-impact perspective.
- 2) Compliance with Password Policy Requirements (Rating 1)
While approximately 1,100 desktop user accounts with update access to GIS records access the system via Citrix, which enforces the standard password requirements, passwords used for a separate application-level login within Citrix are not configured to comply with the standard password requirements and all desktop users utilize their NiSource user ID and a common password for the application-level GIS login. As a result, individual accountability for changes cannot be ensured.
- 3) Removable Media Data Encryption and Distribution (Rating 2)
Processes and controls regarding the security, distribution, and destruction of removeable devices containing offline GIS mapping information monthly are inadequate and not in compliance with Company policy requirements for information classification and protection.
- 4) GIS Disaster Recovery and Business Continuity Controls (Rating 2)
Processes and controls to ensure the GIS platform can be effectively restored in case of a disruption are not in compliance with Company policy and are based upon legacy criticality and risk determinations that may not be current.

Management's Response

Management agrees with the findings noted during this audit and has provided 23 action items that they developed to address the risks identified. Detailed action plans are included in Appendix B. Related to the first finding, GIS Applications management took swift action to review the risks and vulnerabilities related to GIS and has developed action plans, in conjunction with Cybersecurity and Infrastructure management, to address the identified vulnerabilities and implement processes to regularly obtain, review, and address application-related risks and vulnerabilities; key mitigation steps will be implemented by April 2023. Related to the second finding, GIS Applications management has already deployed enforcement of password complexity requirements when passwords have changed or expired; additional mitigation steps to configure passwords expiration and secure passwords used by external service providers will be implemented by July 2023.

Internal Audit Follow Up

Management has provided action plans for all findings with a rating of "1", "2", or "3". We have reviewed management's action plans and believe that the action plans will adequately address the findings identified in this audit. We will track the progress of resolution and will conduct follow-up testing for all rated "1" audit findings and a sample of rated "2" and rated "3" audit findings.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Report *****

"1" Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company's reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

"2" Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

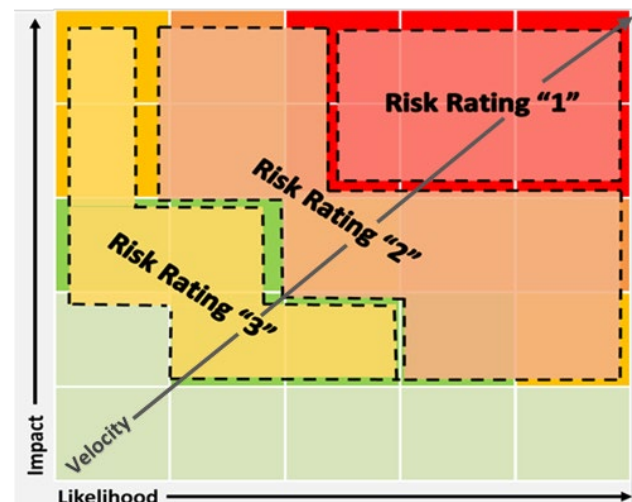
- More than remote probability for damage to the Company's reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

"3" Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited, and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

"4" – Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited



1) <u>Geographic Information System (GIS) Application Risk and Vulnerability Analysis</u>	Rating: 1
<u>Risk:</u> Potential that unevaluated and unaddressed technology vulnerabilities increase cybersecurity risk by enabling entry points to the corporate network; also, potential for unevaluated and unaddressed technology vulnerabilities to increase risk associated with GIS application unavailability and/or GIS data integrity/confidentiality.	
<u>Observation:</u> NiSource Inc. (NiSource or the Company) monitors cybersecurity vulnerabilities using the Qualys platform. Risks and vulnerabilities associated with GIS may be identified during Qualys scans. Additionally, the Innovation Compliance and Risk team maintains a list of known and evaluated IT-related risks and vulnerabilities, some of which relate to GIS. Processes to evaluate risks and vulnerabilities are not formalized for some applications, including the GIS application. Some of the risks and vulnerabilities associated with GIS were not being reviewed on a regular basis by the GIS Applications, Asset Knowledge Management, Cybersecurity, or Innovation Compliance and Risk teams. As a result, risks and vulnerabilities related to the GIS application may not be adequately evaluated and actioned. Over 1,000 risks/vulnerabilities identified during Qualys scans had not been formally assessed by the Cybersecurity, GIS Applications, or the Innovation Compliance and Risk teams and discussed with the GIS application owners from a potential-for-business-impact perspective. Additionally, while the Innovation Compliance and Risk team was tracking 18 risks related to GIS, these risks were not formally managed in the aggregate by the GIS Applications team and GIS application owners.	<u>Management Action Plan:</u> GIS Applications has evaluated the vulnerabilities identified by the Cybersecurity and Innovation Compliance and Risk teams and determined which items need to be addressed. Cybersecurity will perform the following: • Provide a monthly vulnerability report to the GIS Applications team • Include GIS Applications within the weekly vulnerability meetings GIS Applications will perform the following: • Address the identified vulnerabilities through application patching, referral to IT Infrastructure for infrastructure patching, or work with the Innovation Compliance and Risk team to create a risk registry item if a solution does not exist in patch • Review GIS dependencies outlined with the Configuration Management Database (CMDB) to ensure all related assets have been identified for reporting purposes • Formalize a process to ensure that all identified GIS risks and vulnerabilities are evaluated monthly from an application support and business perspective to determine action plans • Utilize the existing risk management process (Archer) to monitor higher risk vulnerabilities that are not immediately addressed by patching and escalate when accepted remediation timelines are exceeded • Formalize an application patch management plan for GIS IT Infrastructure will perform the following: • Formalize an infrastructure patch management plan for GIS • Address the current known application vulnerabilities identified by GIS Applications

	Formalize a process to address ongoing infrastructure vulnerabilities identified in the filtered monthly vulnerability report <u>Responsible:</u> Diego Castillo, Director IT Applications Jeremy Plante, Director Cybersecurity Ishreth Sameem, Director IT Infrastructure <u>Resolution Date:</u> The action plans will be completed by April 2023.
<u>Criteria:</u> Processes are sufficient to ensure that risks and vulnerabilities related to the GIS application are evaluated and appropriately addressed.	
2) <u>Compliance with Password Policy Requirements</u>	Rating: 1
<u>Risk:</u> Potential that system availability is compromised and/or that data integrity is compromised, resulting in negative business consequences.	
<u>Observation:</u> NiSource's policy on identification and access management specifies password complexity requirements and requirements for individual user identification (ID) and passwords. Required password standards are not enforced for GIS users accessing the application from their desktops, including users with privileged accounts (e.g., database administrators). While desktop users access GIS via Citrix, which enforces the standard password requirements, passwords used for a separate application-level login within Citrix are not configured to comply with the standard password requirements. Approximately 1,100 user accounts have update access to GIS records using the GIS desktop application. All desktop users utilize their NiSource user ID and a common password for the application-level GIS login. As a result, individual accountability for changes cannot be ensured.	<u>Management Action Plan:</u> In February 2023, GIS Applications deployed into production enforcement of password complexity requirements when passwords are changed or have expired to meet the minimum corporate standards. Additionally, GIS Applications will perform the following: - Configure a password expiration to remove all shared passwords - Store the Spatial Database Engine (SDE) service account password used by external service providers in CyberArk following the migration to HANA <u>Responsible:</u> Diego Castillo, Director IT Applications <u>Resolution Date:</u> Password expiration will be configured by March 2023. The SDE service account password will be stored in CyberArk by July 2023.
<u>Criteria:</u> Controls are sufficient to ensure that access to GIS data and system functionality is appropriately restricted, including compliance with the Company's password complexity requirements.	

3) <u>Removable Media Data Encryption and Distribution</u>	Rating: 2
<u>Risk:</u> Potential that sensitive information regarding critical infrastructure may be disclosed to unauthorized individuals.	
<u>Observation:</u> The mapping information maintained within GIS is identified as “Highly Restricted” per the Company’s policy on information classification and protection. Therefore, the data are required to be secured, maintained in safe and secure locations, securely transported, and destroyed when no longer needed. Field employees and contractors utilize GIS to locate and identify assets within the field for repair and emergency maintenance. As a result of inconsistent mobile device service to access mapping data through Field Maps, GIS Applications provides approximately 1,000 digital versatile disc (DVD) and universal serial bus (USB) drives with current, location-specific, offline mapping information monthly. Processes and controls regarding the security, distribution, and destruction of these devices are inadequate and not in compliance with policy requirements; specifically: • The distributed DVDs are unencrypted; while the ArcReader application is required to view the data in a map format, the data is viewable without the ArcReader application in a readable database format • While the distributed USB drives are encrypted, the password used is not periodically modified • The DVDs and USB drives are sent via the United States Postal Service • A process to ensure chain of custody for the distributed DVDs/USB drives is not formalized; specifically, DVDs are not tracked and, while USB drives are tracked, only approximately 25% are returned each month	<u>Management Action Plan:</u> Asset Knowledge Management will perform the following: • Evaluate all GIS data practices in consideration of requirements specified in the Information Classification and Protection Policy GIS Applications will perform the following: • Discontinue the distribution of unencrypted removable media for internal users and external contractors • Formalize a process for external contractors to secure the devices in line with policy requirements (including distribution, return, and disposal) until removable media is no longer required <u>Responsible:</u> Diego Castillo, Director IT Applications Aaron Boeke, Director Asset Knowledge Management <u>Resolution Date:</u> The distribution of unencrypted removable media will be discontinued by May 2023 for internal users and July 2023 for external contractors. The GIS data practices evaluation and establishment of a process to secure devices will be completed by July 2023.
<u>Criteria:</u> Processes are sufficient to ensure that sensitive information is appropriately protected as required per Company policy.	
4) <u>GIS Disaster Recovery and Business Continuity Controls</u>	Rating: 2
<u>Risk:</u> Potential that GIS applications are unable to be recovered in the event of a disruption, resulting in unacceptable downtime or failure to restore the application.	
<u>Observation:</u> NiSource’s policy on IT business continuity and disaster recovery outlines requirements to ensure applications can	<u>Management Action Plan:</u> Asset Knowledge Management will:

be restored and business operations can continue in case of a service disruption, including the creation of a business risk assessment and business impact analysis for critical applications and the formalization and periodic testing of a business continuity and disaster recovery plan.

A formal business impact analysis has not been performed for GIS platform, which includes 32 applications. While the GIS applications have each been assigned a criticality tier, the current categorization is based on legacy criticality and risk determinations that may not be current. Additionally, a disaster recovery plan is not formally documented for GIS.

While five of the 32 GIS applications were tested and successfully recovered during the December 2022 disaster recovery exercise, the determination of which specific GIS applications to include in the exercise was not based on a documented criticality assessment that includes consideration of interdependent components of the GIS platform but was based on informal determination of component-level criticality and risk.

- Conduct a formal business risk assessment and business impact analysis for the GIS applications in line with the requirements outlined within the IT Business Continuity and Disaster Recovery Policy
- Formalize and document a business continuity plan in line with the requirements within the IT Business Continuity and Disaster Recovery Policy
- Formalize a process to periodically review the risk assessment, business impact analysis, business continuity, and disaster recovery plans and update as appropriate

GIS Applications will perform the following:

- Document a GIS-specific disaster recovery plan leveraging the existing infrastructure recovery plan
- Re-evaluate the disaster recovery recovery methods criteria for all GIS applications and perform a risk and criticality assessment, including consideration of interdependent components of the platform, to evaluate whether current recovery criticality and critically tiering is appropriate

Responsible:

Diego Castillo, Director IT Applications
Aaron Boeke, Director Asset Knowledge Management

Resolution Date:

The action plans will be completed by July 2023.

Criteria:

Processes and controls are sufficient to ensure that GIS applications can be recovered within an appropriate timeframe in the event of a disruption and that business continuity can be maintained during the period of time that GIS unavailable.



Internal Audit Department



We exist to deliver safe, reliable energy that drives value to our customers

Source to Pay General Controls

Internal Audit Report

Distribution

Respondents:

Adolfo Acevedo Beristain
Heather Bauer
Doug DeBaltzo
Kristen King
Crystal Miller

Beneficiaries:

Sandra Brummitt
Gunnar Gode
Robert Kandell

For Information:

Shawn Anderson
Melanie Berman
Melody Birmingham
Donald Brown
Kim Cuccia
William Jefferson
Lloyd Yates

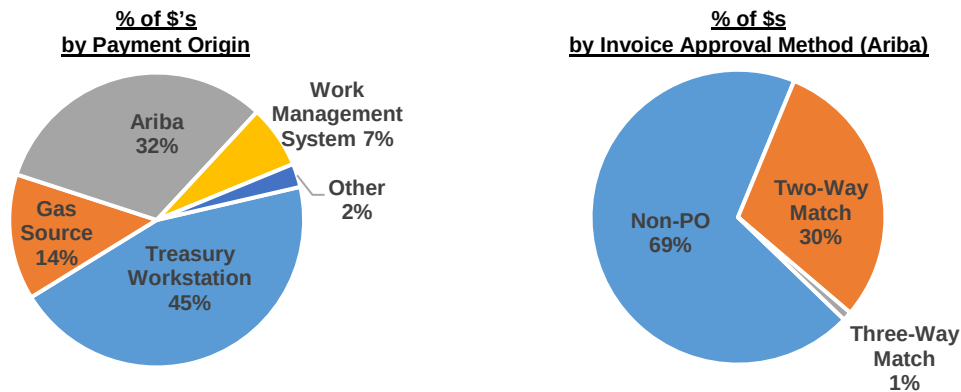


Internal Audit Report

Background

The centralized Supply Chain and Accounts Payable functions within NiSource Corporate Services Company (NCS), a wholly owned subsidiary of NiSource Inc. (NiSource or the Company), manage source to pay activities for all NiSource subsidiaries. The Company's total negotiable spend was \$2.4 billion for 2021 and \$3.0 billion for 2022. The accounts payable balances averaged \$697.8 million during 2021 and \$899.5 million during 2022.

During the 12-month period from August 1, 2021, to July 31, 2022, payments of approximately \$11.6 billion were recorded through PeopleSoft from 15 different payment origins. Most invoices processed during the same time were processed as non-purchase order (non-PO) invoices, with a small percentage of invoices being subject to the three-way match process.



The Supply Chain team is responsible for procurement activities, including supplier identification and management, contract negotiations and approvals, as well as requisition and purchase order support. The Accounts Payable team is responsible for invoice processing and payment, and vendor master file management.

Audit Objective, Approach, and Coverage

The objective of this risk-based internal audit was to provide an independent evaluation of the adequacy, effectiveness, and efficiency of controls associated with the source to pay activities. We completed a risk assessment and conducted detailed process assessments and sample-based transactional testing in higher-risk areas. The review period associated with the procurement activities evaluated during this audit was January 2021 through April 2022 and the review period for accounts payable activities was August 2021 through July 2022.

During the audit, we specifically evaluated:

- Source to pay governance, including policies and procedures and oversight of outsourced third-party performance
- Supplier source activities, including processes related to the identification and selection of vendors
- Procurement process controls, including purchasing documents requirements, authorization, two/three-way match system functionality
- Monitoring activities, including open purchase orders, blanket purchase orders, and payment exceptions
- Vendor master file management, including user access controls and master file additions and changes
- Invoice processing and payment execution within Ariba and the Work Management System (WMS)
- Associated accounting processes related to ensuring accounts payable is correctly recorded
- Segregation of duties
- System interfaces, specifically EDM to Ariba and Ariba and WMS to PeopleSoft

Our audit evaluation was focused on activities managed through Ariba and WMS. During this audit, we did not evaluate processes associated with payments originating from employee expense reports, Gas Source, and Treasury Workstation because these processes were recently evaluated in different audits. Also, we did not test processes associated with systems for which that total spend was determined to be immaterial for the period under audit review (MAPPS, Fleet Card, DIS, CIS, DSM, AEP, Team Connect, Lease System, One Card, Payroll Garnishments, Property Tax, PCard and Telecom).

Internal Audit Finding Ratings

We assign ratings to audit findings based on the following scale (see the Internal Audit Finding Rating Scale in Appendix A):

“1” – Significant Improvement is Needed and Prompt Management Attention is Required

“2” – Improvement is Needed and Management Attention is Necessary

“3” – Some Improvement is Needed and Management Attention is Justified

“4” – Management Evaluation is Desirable

Internal Audit Conclusion and Summary of Observations

Activities related to the source to pay cycle were recently aligned under common leadership to enable process consistency and efficiency, and the combined Source to Pay team rolled out a new source to pay policy in January 2023, which will facilitate consistency objectives. We recommend that the Source to Pay team consider enhancing the policy guidance with specific direction to drive compliance with process expectations.

The newly formed Source to Pay team is developing communication protocols that will be imperative to effectively managing the end-to-end source to pay cycle. We recommend that the team strive to obtain visibility to and understanding of source to pay activities occurring across the entire enterprise. During our review, we particularly noted that the Accounts Payable team would benefit from gaining additional visibility into Northern Indiana Public Service Company (NIPSCO) payables activities.

While the Company has implemented components of the SAP Ariba solutions, NiSource is not using the platform to its full capabilities. Also, the current system configuration can be enhanced to automate control activities and drive process compliance. We recommend that management consider Ariba configuration enhancements to automate higher impact controls and consider enabling additional capabilities in Ariba, especially capabilities related to contract management, as funding becomes available.

Overall, we found that processes and controls related to the source to pay activities (as specified in the “Audit Objective, Approach, and Coverage” section of this report) can be improved. We identified one finding related to vendor master file controls that requires management’s prompt attention (Rating 1). We also identified six findings where management’s attention is necessary (Rating 2) and one finding where management’s attention is justified (Rating 3). In addition, we observed some less-significant items that were discussed with management during the course of the audit.

A summary of audit findings rated “1” through “3” follows (see the Internal Audit Findings Matrix in Appendix B):

- 1) **Vendor Master File Controls** (Rating 1)
Controls are insufficient to ensure changes to the vendor master file are valid, complete, and accurate; specifically: established controls are not being adequately executed; monitoring control execution is not sufficient to ensure changes are appropriately supported; and control design is not sufficient to ensure all key changes are subject to review.
- 2) **Purchasing Document Guidance and Controls Framework** (Rating 2)
Source to pay policies and procedures, as well as systematic and monitoring controls, should be improved to ensure spend is appropriately approved and payment processes are controlled and efficient.
- 3) **Supplier Sourcing and Competitive Bidding Processes** (Rating 2)
Processes are insufficient to ensure vendors are subjected to an appropriate supplier selection process and that related appropriate supporting documentation is retained as required per policy.

- 4) Vendor Contract Administration and Monitoring (Rating 2)
Processes associated with contract maintenance and monitoring are insufficient to ensure that incurred vendor spend aligns with the contracted terms.
- 5) Invoice Exception Monitoring (Rating 2)
Invoice exception monitoring processes are insufficient to ensure timely vendor payments.
- 6) Sarbanes-Oxley (SOX) Control Validation Related to Ariba Automated System Functionality (Rating 2)
Some key controls automated within Ariba have not been subject to periodic testing to ensure the controls were not modified and continue to operate effectively.
- 7) Confidential Information Protection (Rating 2)
Confidential information associated with payroll garnishments is not protected per policy.
- 8) Sufficiency of Metric Monitoring for Outsourced Processes (Rating 3)
Processes related to some Tata Consultancy Services (TCS) performance metrics are insufficient.

Management's Response

Management agrees with the findings noted during this audit and has provided action plans to address the risks identified. Detailed action plans are included in Appendix B. The key mitigation steps will be completed by December 2023.

Internal Audit Follow Up

Management has provided action plans for all findings with a rating of "1", "2", or "3". We have reviewed management's action plans and believe that the action plans will adequately address the findings identified in this audit. We will track the progress of resolution and will conduct follow-up testing for all rated "1" audit findings and a sample of rated "2" and rated "3" audit findings.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Report *****

"1" Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company's reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

"2" Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

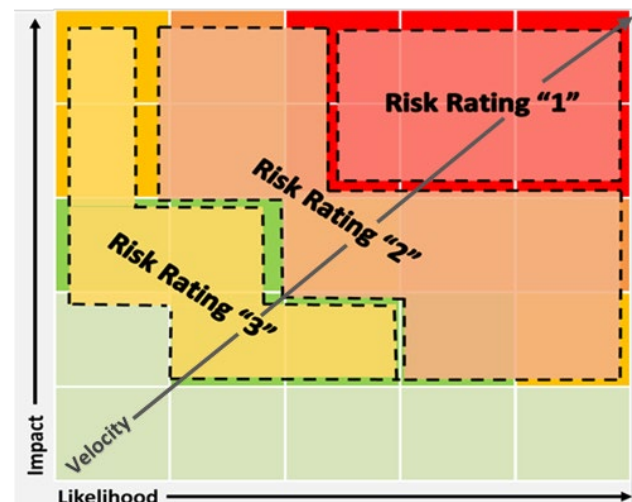
- More than remote probability for damage to the Company's reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

"3" Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

"4" – Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited



1) <u>Vendor Master File Controls</u>	Rating: 1
<u>Risk:</u> Potential for financial loss resulting from payments remitted to incorrect payees caused by erroneous or fraudulent vendor master file information.	
<u>Observation:</u> Key vendor information, including banking information, supplier contact information, address, and agreed upon payment terms, is maintained within the PeopleSoft vendor master file. Changes to vendor master file data are processed by Tata Consultancy Services (TCS). Controls to ensure the completeness and accuracy of key vendor master file data are not sufficient; specifically: • While a Sarbanes-Oxley (SOX) control has been established to periodically review bank account changes within the vendor master file, the control procedures were not required per the TCS standard operating procedures (SOP) resulting in the control not being executed during the audit period until September 2022 • The report used to monitor bank account changes does not systematically identify all changed data fields and only includes the most recent modification date (versus all change dates) • Acceptable documentation to support changes to vendor information and records retention requirements are not defined within the TCS SOPs; also, changes are sometimes processed without support or using modifiable supporting documents; we evaluated a sample of 40 changes to banking information and evidence supporting the accuracy of changes was not provided for 18 (of 40) changes and evidence supporting appropriate approval was not provided for four (of 40) changes • The current process allows changes to be made directly in the vendor master file, circumventing the initial change review process • The defined vendor master file SOX control only requires bank account changes to be reviewed and does not require other key vendor information, including payment terms, to be reviewed	<u>Management Action Plan:</u> The SOX control was executed from September – December 2022; management completed SOX testing of this control in Q4 2022 and did not identify any transactional exceptions. To enhance the vendor master file maintenance process governance, Accounts Payable management will perform the following: • Update vendor master file maintenance policies and SOPs to include required execution of the weekly review of vendor changes, define acceptable documentation to support changes to vendor information, and require obtaining and retaining supporting documentation for changes in line with the Company's record retention requirements; policy updates will be made in coordination with overall NiSource master data management and data governance policies • Work with SOX Compliance management to review the financial reporting risks associated with additional key vendor updates and update the requirements of the existing SOX control accordingly • Retrain the TCS vendor maintenance team on the updated SOPs and control requirements • Execute a one-time vendor master file cleanup To improve system functionality and reporting associated with the vendor master file, Accounts Payable management will work with Information Technology (IT) to develop and execute a plan to systematically track the reasons for vendor master file updates, limit the ability to make changes directly within the vendor master file, and enhance reporting capabilities. <u>Responsible:</u> Adolfo Acevedo Beristain, Director of Accounts Payable <u>Resolution Date:</u> The updates to the vendor master file policies, SOPs, and SOX control requirements, as well as execution of related trainings, will be completed by June 2023. The one-time vendor master file cleanup will be completed by December 2023.

	A plan to address system functionality and reporting elements will be developed by June 2023; dates associated with specific action steps to be identified in the plan are to be determined.
<u>Evaluation Criteria:</u> Processes and controls are sufficient to ensure changes to the vendor master file are properly authorized and reviewed; specifically: 1) a process has been formalized and documented to ensure changes to vendor master file information are subject to appropriate review and approval and appropriate supporting documentation has been defined; 2) a process has been formalized and documented to periodically monitor and review key changes to vendor master file information to ensure the changes are accurate and supported by appropriate documentation; and 3) the report to identify key changes to vendor master file information is configured to pull all key vendor changes.	
2) <u>Purchasing Document Guidance and Controls Framework</u>	Rating: 2
<u>Risk:</u> Potential that fraudulent purchasing and or payment transactions are not prevented or timely detected and potential for increased costs and inaccurate financial reporting.	
<u>Observation:</u> NiSource Inc.'s (NiSource or the Company) source to pay policies and procedures, as well as systematic and monitoring controls should be improved to ensure spend is appropriately approved and payment processes are controlled and efficient; specifically: • Ariba is not configured to prevent invoices from being applied against a purchase order that was approved after the corresponding invoice date and this scenario is not monitored; payments totaling \$43.7 million were associated with invoices dated prior to the creation of the related purchase orders during 2022 • The source to pay policy specifies purchasing process requirements that ensure approval of spend at the time of commitment, as well as drive automated payment processing that is controlled and efficient, but invoice approval method (i.e., non-purchase order versus two/three-way match) compliance targets are not defined or monitored • The source to pay policy does not provide specific guidance regarding when purchasing agreements are required versus not required and which purchasing documents are appropriate for which types of purchasing transactions; the policy also does not provide specific guidelines regarding blanket purchase orders and blanket purchase order activities are not monitored • Open purchase orders are not monitored to ensure they are appropriately closed to prevent unrelated or fraudulent spend from being inappropriately applied • Ariba is not configured to require acknowledgement that services have been rendered prior to invoices	<u>Management Action Plan:</u> To enhance purchasing document governance and compliance monitoring, Supply Chain management will perform the following: • Modify the source to pay policy to clarify expectations around the use of purchasing documents, including blanket purchase orders • Conduct a read and acknowledge training on the revised source to pay policy for the entire Company • Update the current Ariba training to incorporate relevant policy updates • Formalize a process to periodically monitor spend by invoice approval methods • Formalize a process to periodically review open purchase orders and close long outstanding purchase orders as applicable To improve the system functionality and reporting associated with the invoice matching process, Supply Chain management will work with IT to develop and execute a plan to systematically drive compliance with purchasing document requirements. <u>Responsible:</u> Crystal Miller, Director of Supply Chain Strategy & Analytics <u>Resolution Date:</u> The source to pay policy updates will be executed and the related trainings will be updated and rolled out by August 2023. The formalization of the processes to monitor spend

being processed via a two-way match for payment	by invoice approval methods and review open purchase orders will be completed by June 2023. A plan to address system functionality and reporting elements will be developed by August 2023; dates associated with specific action steps to be identified in the plan are to be determined.
<u>Evaluation Criteria:</u> Supply Chain processes and controls are sufficient to ensure Company spend is appropriately controlled and assessed based upon the nature of the transaction; specifically: 1) purchasing expectations and requirements, including when to use appropriate sourcing documents (e.g., blanket purchase orders), have been formalized within a company policy that is communicated to employees; 2) system functionality is in place to prevent invoices from being matched against purchase orders created after the invoice date; 3) system functionality requires the receipt of goods and/or services within the system prior to invoice payment; 4) monitoring activities have been established to review spend by approval type to identify potential non-compliance with policy; and 5) monitoring activities have been established to review open purchase orders for potential mis-use.	
3) <u>Supplier Sourcing and Competitive Bidding Processes</u>	
<u>Risk:</u> Potential for increased costs and risk related to poor supplier performance and potential that supplier quality performance and diversity demographics do not align with Company objectives.	
<u>Observation:</u> The source to pay policy requires that vendors with significant spend (\$100,000 under the updated policy as of January 2023 and \$250,000 prior to January 2023) be subjected to a supplier selection process. However, the policy does not define consideration of aggregate commitment, and a process is not defined to identify vendors with aggregate spend over the policy threshold for which a required supplier selection process has not occurred. In addition, evidence supporting appropriate execution of the required supplier selection process is not always maintained as required per the records management policy (retention requirement of six years). We requested supplier selection documentation for nine suppliers with spend above the applicable source to pay policy threshold, and evidence of appropriate process execution was not available for four (of nine) suppliers.	<u>Management Action Plan:</u> To enhance supplier sourcing governance and compliance monitoring, Supply Chain management will perform the following: • Update the source to pay policy to define aggregate commitment and its application by vendor • Formalize a process to monitor vendor spend over the threshold outlined within the source to pay policy for instances where vendors were not subject to supplier selection processes • Formalize a process to maintain evidence of executed supplier selection processes as required per the records management policy (i.e., six years) • Conduct applicable training on supplier sourcing documentation records retention requirements To improve the system functionality and reporting associated with supplier sourcing and competitive bidding, Supply Chain management will work with IT to develop and execute a plan to systematically enhance requirements within the process. <u>Responsible:</u> Crystal Miller, Director of Supply Chain Strategy and Analytics

	<u>Resolution Date:</u> The source to pay policy updates will be executed by August 2023. The formalization of the processes to monitor vendor spend against the sourcing threshold and maintain sourcing documentation, as well as the execution of related training, will be completed by June 2023. A plan to address system functionality and reporting elements will be developed by August 2023; dates associated with specific action steps to be identified in the plan are to be determined.
<u>Evaluation Criteria:</u> Processes and controls are sufficient to ensure appropriate supplier selection processes are executed for vendors with significant spend; specifically: 1) vendor selection methodology and thresholds are established within company policy; 2) anticipated vendor spend over the established threshold is subject to supplier selection methods; 3) formalized process to maintain evidence of executed supplier selection processes has been developed and rolled out; and 4) Supply Chain management periodically monitors vendor spend over the established threshold to identify instances where vendors were not subject to supplier selection processes.	
4) <u>Vendor Contract Administration and Monitoring</u>	Rating: 2
<u>Risk:</u> Potential that misalignment of purchasing activities and contracts result in increased costs and risk.	
<u>Observation:</u> Contract maintenance and monitoring controls are not sufficient to ensure that incurred vendor spend aligns with the contracted terms; specifically: • Ariba is not configured to assess total vendor spend against the associated contracts to identify instances where spend may exceed contractual limits • Ariba is not configured to validate that the terms of purchase orders and/or invoices agree to corresponding contracts, and monitoring activities are not implemented to identify payments that are not in line with contracted terms • The Work Management System (WMS) is not configured to prevent total spend from exceeding the authorized amount per the established contract, and monitoring controls are not established to detect when spend has been incurred over the authorized amount; as of January 2023, 21% of active WMS contracts exceeded the approved contract spend limits • Ariba and WMS are not configured to flag expiring contracts • Ariba and WMS are not configured to flag purchase order terms that are inconsistent with master agreement terms or invoice terms that are inconsistent with contract terms	<u>Management Action Plan:</u> To improve vendor contract administration governance and monitoring, Supply Chain management will perform the following: • Formalize a process to address instances of contract spend non-compliance, including the development of monitoring reports for Ariba and WMS to identify instances when spend exceeds contractual limits • Formalize a process over payment term assignment, including required documentation needed when deviating from standard payment terms • Execute a one-time Ariba Contract Workspace clean-up, including Preferred Supplier expired contracts • Update the source to pay policy to limit and/or prevent the use of non-expiring contracts • Formalize a process to monitor the use of perpetual and evergreen contracts Supply Chain management will work with IT to develop and execute a plan to systematically enhance processes and controls associated with contract related spend, application of payment terms and contract expiration dates.

The current source to pay policy does not prevent the use of perpetual and evergreen contracts and perpetual and evergreen are not actively monitored to ensure appropriate terms and conditions	<u>Responsible:</u> Crystal Miller, Director of Supply Chain Strategy and Analytics <u>Resolution Date:</u> The processes to formalize monitoring of contract spend non-compliance, payment term assignment, and non-expiring/evergreen contracts will be implemented by June 2023. The source to pay policy updates will be executed by August 2023. The Ariba Workspace clean-up activities will be completed by December 2023. A plan will be developed with IT to address system functionality by August 2023; dates associated with specific action steps to be identified in the plan are to be determined.
<u>Evaluation Criteria:</u> Processes and controls are sufficient to ensure contracted spend is appropriate and in line with the underlying agreement; specifically: 1) system functionality is in place to assess total spend against the associated contracts; 2) system functionality is in place to validate the terms of purchase orders and/or invoices against the underlying contract; 3) system functionality is in place to prevent total spend from exceeding the authorized amount per the underlying contract; 4) system functionality or monitoring is in place to ensure invoicing is in agreement with current contracted terms; and 5) Company policy has been established to discourage the use of non-expiring contracts.	
5) <u>Invoice Exception Monitoring</u>	
<u>Risk:</u> Potential that unpaid invoices result in financial penalties and negative reputational impact with vendors.	
<u>Observation:</u> Invoice exceptions occur when an invoice is submitted for processing and fails to meet the two- or three-way match automated process requirements within Ariba. Exceptions must be reviewed and cleared to be processed for payment. Invoice exception processes are not sufficient; specifically: - Invoice exceptions for Northern Indiana Public Service Company (NIPSCO) are not monitored and reviewed - An invoice exception review process for NiSource Corporate Service Company (NCS) and Columbia Gas Distribution Companies (CGC) was implemented beginning June 2022 but was not formalized; as a result, evidence of process execution is inconsistent - Controls to ensure the completeness and accuracy of the weekly, point-in-time report utilized to review the NCS/CGC invoice exceptions are inadequate; during our transactional testing we identified one weekly report that was incomplete	<u>Management Action Plan:</u> Accounts Payable management will perform the following: - Develop and execute a plan to formalize the Ariba invoice exceptions process for NCS/CGC, including maintaining evidence of control execution, implementation of a formal follow-up process to ensure that exceptions are worked in a timely manner, and maintaining evidence of logic used to run the report to support the completeness and accuracy of the reporting - Develop and execute a plan to formally monitor and review Ariba invoice exceptions at NIPSCO, including maintaining evidence of control execution, implementation of a formal follow-up process to ensure exceptions are worked in a timely manner, and maintaining evidence of logic used to run the report to support the completeness and accuracy of the reporting <u>Responsible:</u> Adolfo Acevedo Beristain, Director of Accounts Payable

Resolution Date:

The plans to formalize invoice exceptions monitoring at NCS/CGC and to formally monitor and review Ariba invoice exceptions for NIPSCO will be developed by June 2023; dates associated with specific action steps to be identified in the plans are to be determined.

Evaluation Criteria:

Processes and controls are sufficient to ensure that invoices that fail the two- or three-way match process in Ariba are monitored and reviewed, specifically: 1) reporting is developed to identify any invoices that fail the match processes; 2) the report is formally reviewed periodically, including a review of report completeness and accuracy; 3) invoice exceptions are actively worked to resolution in a timely manner; and 4) evidence of the review is documented and maintained.

6) Sarbanes-Oxley (SOX) Control Validation Related to Ariba Automated System Functionality

Rating: 2

Risk:

Potential that unidentified automated system functionality control changes lead to errors not being prevented or timely detected.

Observation:

The source to pay activities rely upon automated system functionality within Ariba to execute key controls that ensure vendors are paid appropriately and accurately, including matching invoices against purchase orders and routing invoices and vendor master file changes for approval. While these controls have been identified and included within the relevant business process SOX control framework, they have not been subject to periodic testing to ensure the controls are operating effectively as intended and ensure the underlying system configuration has not been inappropriately or inadvertently changed since initial system implementation.

Management Action Plan:

SOX Compliance, Accounts Payable, and Innovation Compliance and Risk management will perform the following:

- Develop a formal process and review control for periodic evaluation of Ariba change logs
- Develop policy guidelines for periodic Ariba functionality benchmark testing to be executed
- Formalize and execute the testing/review as part of the SOX testing framework

Responsible:

Adolfo Acevedo Beristain, Director of Accounts Payable
Heather Bauer, Director Compliance
Kristen King, Director Consolidations, External Reporting, Technical Accounting, & SOX

Resolution Date:

The process and policy guidelines updates will be implemented by June 2023. As part of the Q3 2023 SOX control testing cycle, the system functionality testing will be executed and reviewed by October 2023.

Evaluation Criteria:

Controls and processes are sufficient to ensure that the Ariba system has been appropriately configured to perform key source to pay processes, specifically: 1) system configuration is tested at the time of system implementation; 2) system audit logs are reviewed annually to identify any changes impacting key system functionality; 3) identified changes to system functionality are tested; and 4) system configurations that have not been updated are subject to periodic (e.g., every three years) benchmark testing.

7) <u>Confidential Information Protection</u>	Rating: 2
<u>Risk:</u> Potential for exposure of confidential employee information to inappropriate parties, resulting in financial loss and reputational impact.	
<u>Observation:</u> Human Resources (HR) and payroll information is identified as "Highly Restricted" per the Company's policy on information classification and protection. Therefore, the data is required to be secured, maintained in safe and secure locations, securely transported, and destroyed when no longer needed. Confidential information utilized by HR to prepare payroll garnishments is not appropriately protected as required per policy when the associated information is sent to other functions to record and process.	<u>Management Action Plan:</u> Accounts Payable management will work with HR to develop and execute a plan to limit the unsecured distribution of confidential information related to payroll garnishments that is in line with the requirements of the Information Classification and Protection policy. <u>Responsible:</u> Adolfo Acevedo Beristain, Director of Accounts Payable <u>Resolution Date:</u> Accounts Payable management will partner with HR to develop a plan by June 2023; dates associated with specific action steps to be identified in the plan are to be determined.
<u>Evaluation Criteria:</u> Controls and processes are sufficient to ensure confidential employee information is appropriately protected, specifically: 1) payroll garnishment information provided from HR to Accounting and Accounts Payable for processing is limited to only the baseline information needed to process payment; 2) sensitive payroll garnishment information is transmitted from HR to Accounting and Accounts Payable in a confidential manner in line with Company policy requirements; and 3) distribution of sensitive payroll garnishment is limited based upon roles and responsibilities.	
8) <u>Sufficiency of Metric Monitoring for Outsourced Processes</u>	Rating: 3
<u>Risk:</u> Potential that vendor performance not in line with Company expectations goes undetected, resulting in missed penalty enforcement and financial loss.	
<u>Observation:</u> Transactional processing of certain source to pay activities has been outsourced to TCS. Various metrics, including key performance indicators (KPI) and service level agreements (SLA) have been established within the contract to measure the performance of the work performed by TCS and are monitored by the Accounts Payable department and the Contract Governance team. However, the performance metrics are not sufficient to ensure transactional processing is performed in line with Company expectations; specifically: • The expected and minimum service levels for one KPI are being measured at the same percentage • One SLA metric was incorrectly calculated, therefore actual performance has not been communicated • TCS does not always provide sufficient evidence to support their performance of some metrics	<u>Management Action Plan:</u> Accounts Payable and Contract Governance management will perform the following: • Perform an evaluation over the current TCS SLAs and KPIs within the contract in place to determine if any revisions are appropriate; if revisions are necessary, the contract will be modified with the vendor to reflect the updated expectations • Formalize the TCS SLA and KPI review process to include a review of the underlying calculations to ensure they are complete and accurate • Formalize the quality control expectations and requirements for TCS related to the execution of accounts payable transactions and document this updated guidance within the SOP • Conduct training with TCS on the updated SOPs

- The SOPs provided to TCS related to quality reviews executed for processing performed by other TCS associates do not provide an appropriate level of guidance regarding the quality control review requirements expected to be performed on the supporting documentation submitted to NiSource in order to determine that the SLA accuracy measurements are being met

Responsible:

Adolfo Acevedo Beristain, Director of Accounts Payable
Doug DeBaltzo, Director of Indirect Category Management
Crystal Miller, Director of Supply Chain Strategy and Analytics

Resolution Date:

The review of the SLAs and KPIs, including the implementation of any necessary contract adjustments, will be completed by August 2023.

The SLA and KPI review process will be formalized by June 2023.

The updates to the SOPs, as well as execution of related training, will be completed by August 2023.

Evaluation Criteria:

Processes and controls are sufficient to ensure outsourced vendor processing is in line with Company expectations established over the negotiation and monitoring of third-party service provider contracts; specifically: 1) SLAs and KPIs addressing the work outsourced to the vendor have been identified and agreed upon within executed contracts; 2) the required supporting evidence provided to substantiate the third-party service providers performance is provided and reviewed periodically to ensure performance is in line with expectations and the information provided to support the SLAs and KPIs is complete and accurate; and 3) Monitoring and reporting is in place to communicate and take appropriate action, per contracted terms, for performance expectations that do not meet requirements.



Internal Audit Department

We exist to deliver safe, reliable energy that drives value to our customers

Cybersecurity – Cloud Computing Controls

Internal Audit Report

Distribution

Respondents:

Jason Griffith
Jeremy Plante
Ishreth Sameem

Beneficiaries:

Waco Bankston
Percell Berry
Carla Donev
Robert Kandell

Other Key Personnel:

Heather Bauer

For Information:

Shawn Anderson
Melanie Berman
Melody Birmingham
Donald Brown
Kim Cuccia
William Jefferson
Lloyd Yates

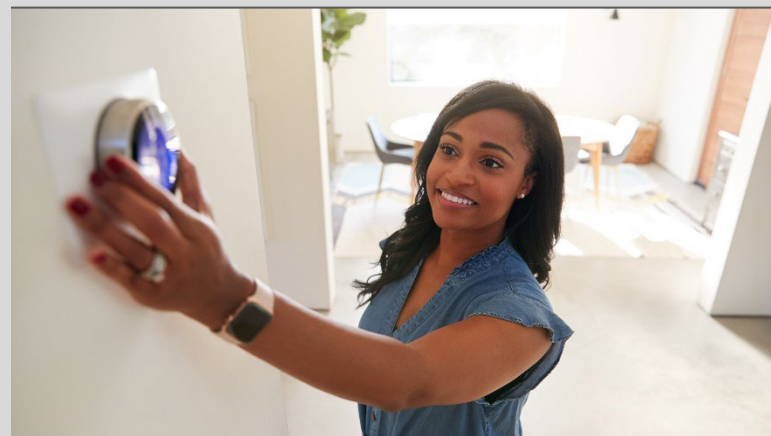
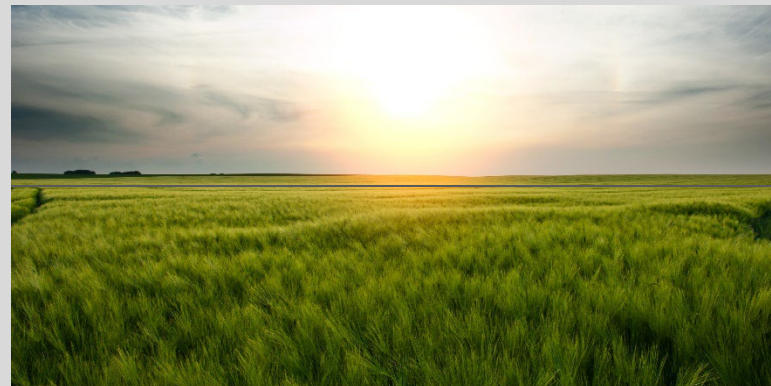
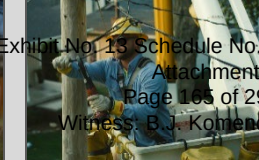


Table of Contents

<u>Executive Summary</u>	4
<u>Initiatives to Focus on & What Good Looks Like</u>	11
<u>Azure Findings Summary</u>	14
<u>AWS Findings Summary</u>	23
<u>Appendix A: Audit Observations Detailed List</u>	33



Executive Summary



Assessment Overview

The purpose of this assessment was to evaluate NiSource's production applications deployed in Amazon Web Services (AWS) as well as non-production environment for the first planned application in Azure. This was accomplished via an automated technical assessment as well as control interviews, both of which levered best practices across Identity and Access Management (IAM), Data Protection, Network and Infrastructure Protection, Logging and Monitoring, and Disaster Recovery. The supporting fieldwork took place from 12/02/2022 through 12/20/2022:

Assessment Approach



Scoped accounts based on **resource richness, complexity, criticality to the business, and footprint coverage**



Connected to 1 Azure subscription and 4 AWS accounts consisting of **25 unique Azure & 91 unique AWS** resource types, **measuring configuration compliance against best practice** policy sets around our five focus control areas.



Conducted interviews assessing Azure and AWS across **Identity and Access Management, Data Protection, Network Security, Logging and Monitoring, and Disaster Recovery**



Consolidated results into a final report **summarizing observations**, detailing **program level recommendations**, and **next steps** towards improving security maturity for cloud

Cloud Environments Covered



Azure

Non-Production cloud platform that will support NiSource's cloud migration efforts



AWS

Multiple production environments which run all of NiSource's AWS workloads

Assessment Outcomes



Technical Scan Results

2k+ compliance results obtained from scanning two cloud platforms against a total of 718 security best practice policies. The document also contains helpful visuals and summarized sheets



Final Report

Captured key takeaways, summarized assessment results, and delivered both low-level tactical and high-level strategic recommendations for NiSource to mature its cloud program

Key Takeaways



High Configuration Compliance

Through a technical review of the environment it was discovered that a high number of resources were adhering to best practices, with Azure resources coming in at 97% compliance and AWS resources 72% compliance.



Lack of Defined Guardrails

While there was a high compliance percentage among existing resources, there are no programmatic guardrails to prevent the deployment of insecure resources in the future. There is also no active configuration monitoring in place.



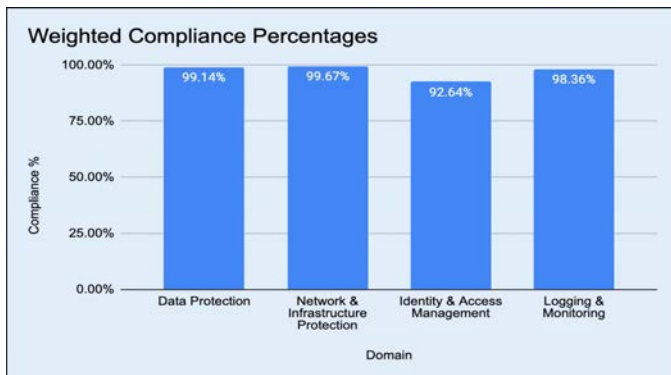
Tooling Underutilization

While there is a Cloud Security Posture Management (CSPM) solution at NiSource, it is not fully utilized and increased usage may highly benefit engineering teams as they build out additional environments.

Cloud Security Technical Compliance by Domain

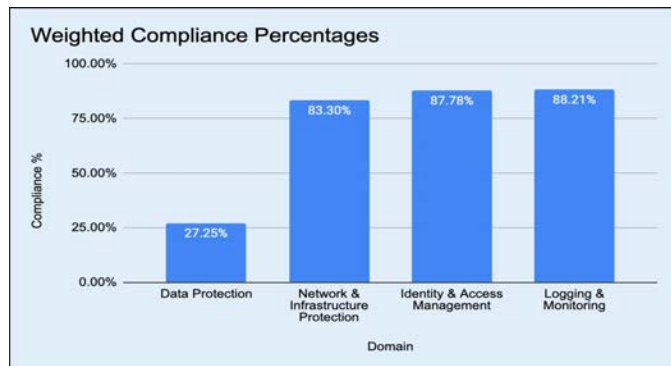
Below is a summary of NiSource's overall cloud compliance by domain along with a summary of strengths and weaknesses for the current cloud security posture:

Azure



Note: The above graph displays overall weighted compliance % across the 4 domains assessed.

AWS



Note: The above graph displays overall weighted compliance % across the 4 domains assessed.

Key Takeaways

Weighted Azure Compliance**97%****Weighted AWS Compliance****72%**

The above compliance percentages are weighted by taking into account resource volumes and risk severity levels



Weighted compliance rates were similar for Azure and AWS, with a total of 85% weighted compliance when averaged together



Network and Infrastructure Protection had high weighted compliance across both Azure and AWS



Data Protection overall had the lowest average policy compliance in AWS, with **27% policy compliance** due to an extremely large amount of old image snapshots



While compliance was very high across the Azure environment, **Identity and Access Management** was the lowest with **92%**



Overall, of the AWS & Azure environments assessed, the AWS environment was less compliant

Interview Based Control Process Observations

Below is a summary of NiSource's overall cloud compliance by domain along with a summary of strengths and weaknesses for the current cloud security posture. Additional details on the ratings levels are included at the end of the executive summary.

Key Takeaways

Total Azure Observations

10

Total AWS Observations

7

The above compliance percentages are weighted by taking into account resource volumes and risk severity levels



Across both AWS and Azure, **Data Protection** had the most observations due to a lack of programmatic guardrails and active configuration monitoring



Identity and Access Management was the most compliant domain across both AWS and Azure



The key Azure observations focused around the **Network Design**, and **Disaster Recovery** capabilities



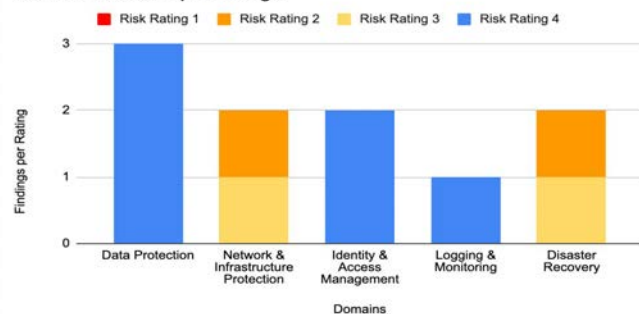
Within AWS the **lack of integration to standard Logging and Monitoring tools** garnered the most attention



Overall, while the Azure environment had more observations, they were mainly **informational**

Azure

Control Workshop Findings



AWS

Control Workshop Findings



Cloud Threat Landscape

Cloud misconfigurations are the new normal, and account for a vast majority of breaches we see in the cloud. While they may seem trivial in nature they often act as a foothold to allow for much more sophisticated and costly attacks which can permeate across an ecosystem.

Landscape Overview



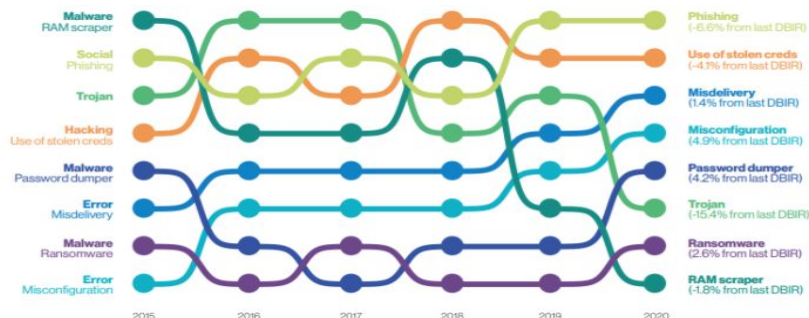
Gartner has predicted that **99% of cloud security failures over the next five years will be caused by user error** – with much of the issue related to configuration issues

Security breaches and incidents resulting from **configuration errors are more common than malware and just behind Social engineering** according to Verizon's 2020 Data Breach Investigations Report



PwC Data Trust Insights survey indicates cloud service providers top the list of 'very likely' threat vectors, while cyber attacks on cloud service top the list of threats that will have 'significantly negative impact'

Misconfiguration errors are trending to a leading cause of cyber incidents



Threat Scenarios

Botnet Malware



A compute instance that is improperly deployed without Web Application Firewall (WAF) protection, may allow for the installation of Malware and communication with an external attacker system.



Ransomware Attack

Ransomware can be planted on an improperly deployed Database which may threaten company operations.



Compromised Cloud Credentials

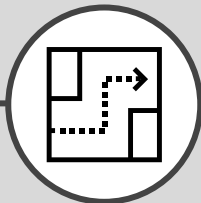
Improper credential rotation or storage can lead to leaked credentials, granting unauthorized access throughout the cloud environment.

Focus Areas for NiSource

Below are three initial focus areas for NiSource to help drive maturity of the cloud organization:

Define Cloud Operating Model

Initial focus area - Proposed for the cloud use case environment



- Formalize a cloud operating model made up of key stakeholders from Engineering & Operations, Enterprise Architecture, Security, Cloud Platform Teams, Compliance, and Third Party Risk Management that defines roles and responsibilities across cloud environments
- Formalize the requirements each group needs in order to remain effective in their respective roles while meeting defined security policies

Enhance CSPM Capabilities

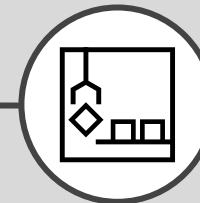
Initial focus area - Developed & Deployed for the cloud use case environment



- Leverage existing toolset to confirm and address existing misconfigurations in the environment
- Cater the CSPM tool to scan against the target control framework to ensure that the configurations in place are in alignment with the framework
- Work closely with engineering teams to provide regular results and enable self-assessments to drive a complete security posture

Application Migration Security

Initial focus area - Utilized for the future planning of the cloud environment



- Review the existing app migration plan and identify different modalities of migration (rehost, refactor, repurchase, etc.)
- Conduct an assessment of existing security tooling and capabilities and whether or not they are sufficient to support migration.
- Ensure the existing toolset can be leveraged to support ongoing security and monitoring for each application migrated to the cloud

Risk Severity Rating

Remediation timelines, descriptions, and associated inherited risks are considered for each severity rating below:

Severity Level: 1



Description: Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company's reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

Severity Level: 2



Description: Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

- More than remote probability for damage to the Company's reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

Severity Level: 3



Description: Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

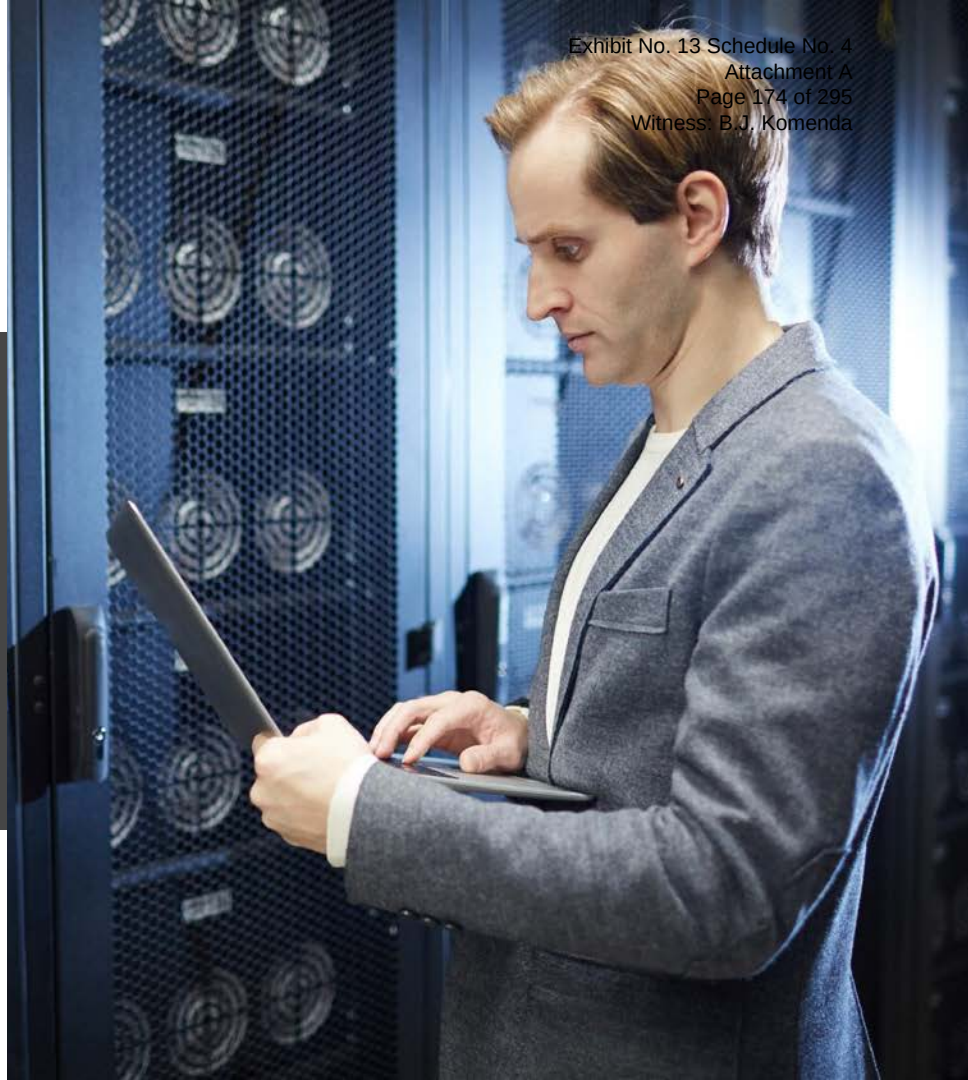
Severity Level: 4



Description: Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited

Initiatives to Focus on & What Good Looks Like



Program Recommendations

Based on the systemic themes identified during PwC's assessment and corresponding analysis, the following recommendations have been suggested for NiSource to increase their program capabilities and consequently achieve cloud security posture management.

Remediation Level of Effort and Level of Benefit

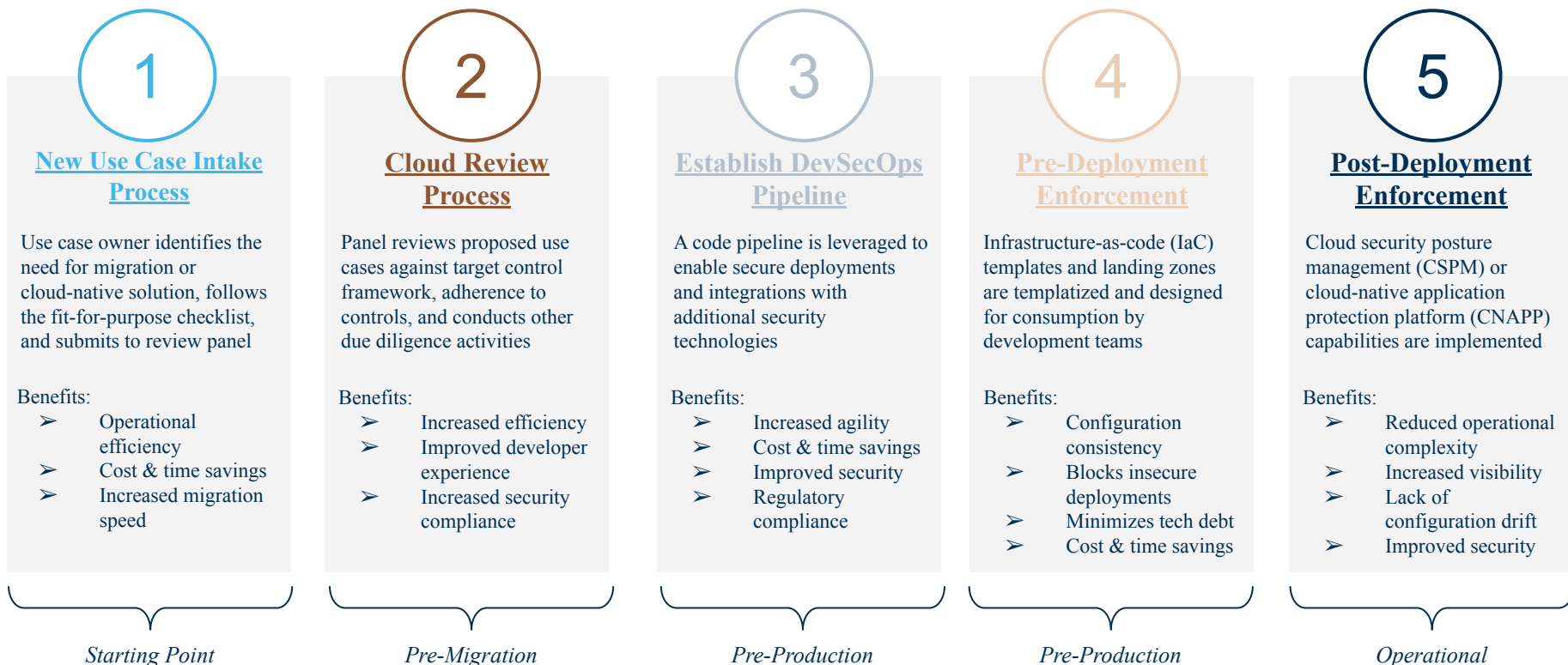
To prevent the build up of additional tech debt it is recommended that NiSource begin remediation with solutions that will prevent security misconfigurations from being deployed and persisting in the environment.

Level of Benefit	High	1, 2	3, 5
	Medium	6	4
	Low		
		Limited	Moderate
		Major	
		Level of Effort	

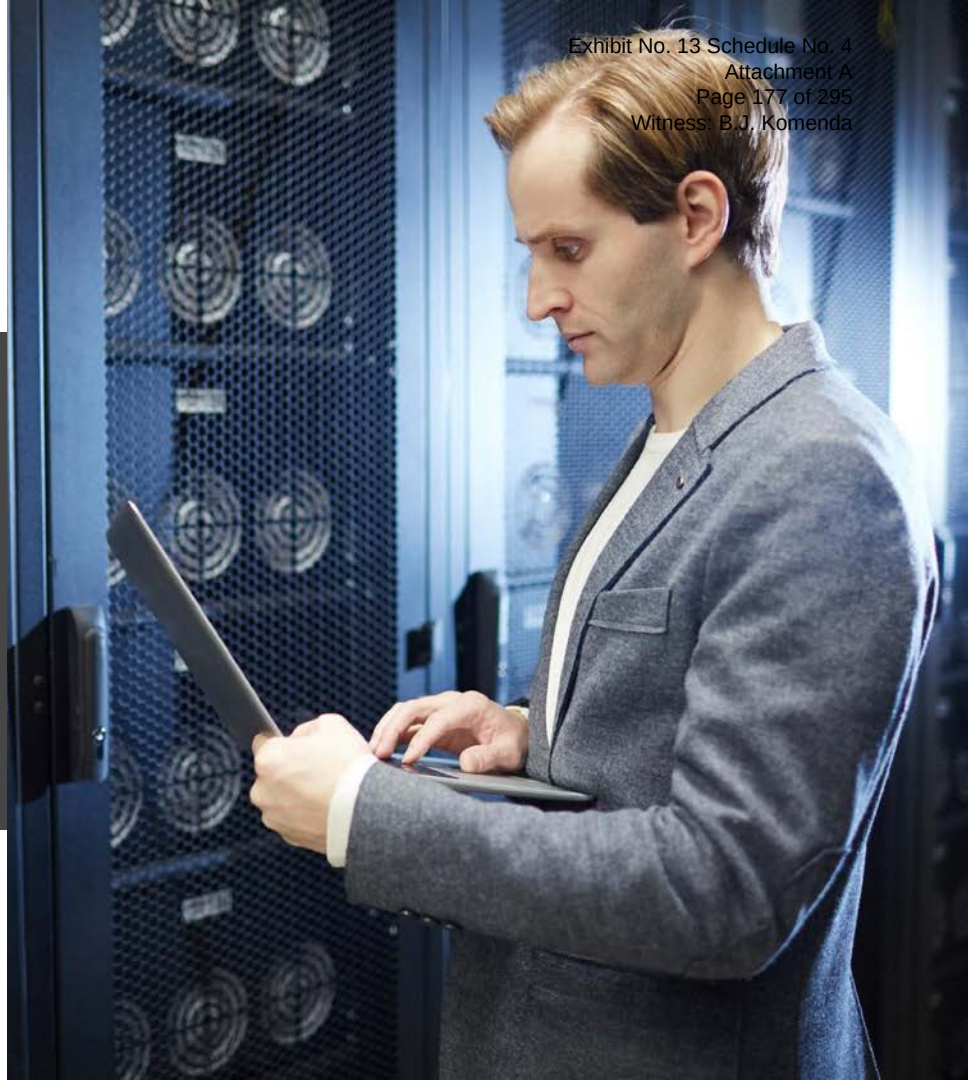
Prioritized Recommendation Summary				
Initiatives		Recommended Initiatives Summary		Recommended Immediate Next Steps
	1	Cloud Operating Model	Generate a cloud operating model to further define roles and responsibilities across all teams for both cloud environments.	- Define all operating responsibilities across the cloud environments - Meet with relevant teams to assign responsibility to various operational aspects
	2	Enhancing CSPM Capabilities	Leverage existing CSPM technologies to buildout full policy set across both cloud environments, mapped to existing NiSource controls.	- Evaluate current NiSource policies which can be adapted to technical cloud policies - Map existing CSPM policies to NiSource policies - Generate custom CSPM policies to fill any policy gaps
	3	Application Migration Security Strategy	Review the existing application migration strategy to identify common migration patterns and potential gaps in security tooling or capabilities to support such migrations.	- Identify the types of migration paths that applications will fall into and what the security requirements for those paths - Conduct a security tools and capabilities assessment to determine gaps that need to be addressed to support migration strategy
	4	Network Segregation (Azure)	Introduce segregation into the Azure network architecture to segregate at a minimum production and non-production from each other.	- Evaluate current network architecture and identify opportunities to implement segregation (lifecycle, application, etc.) - Define network policies and where those policies will be located within the architecture
	5	Disaster Recovery Capabilities (Azure)	Enable Disaster Recovery capabilities within the Azure environment to support requirements for applications being onboarded into Azure.	- Identify the DR and resiliency requirements for applications earmarked to move to Azure - Plan the resource and architecture requirements to support these - Begin to implement the additional architecture needed
	6	Log Centralization (AWS)	Implement the ability to forward logs from the AWS environment to the Splunk environment in order to centralize all cloud security logs into a single place.	- Identify all required log sources within AWS and their current location - Plan and implement architecture to ingest logs into Splunk - Coordinate with security team to confirm they are properly receiving logs

Mature Cloud Lifecycle

Below is an example of what a mature cloud enablement lifecycle looks like for an organization that has heavily adopted cloud and is managing security well:



Azure Findings Summary



Risk Severity Rating

Remediation timelines, descriptions, and associated inherited risks are considered for each severity rating below:

Severity Level: 1



Description: Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company's reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

Severity Level: 2



Description: Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

- More than remote probability for damage to the Company's reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

Severity Level: 3



Description: Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

Severity Level: 4

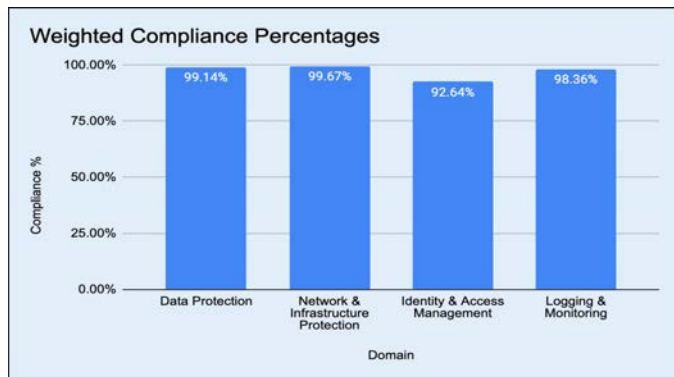


Description: Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited

Technical Results for Azure

The graphs below displays weighted compliance percentages for each of the domains assessed against Azure:



Note: The above graph displays overall weighted compliance % across the 4 domains assessed.

Key Takeaways

- ❖ All domains are highly compliant with an average compliance percentage of 97%
- ❖ Identity & Access Management is the lowest domain, but is still above 90% complaint

Positive Scan Findings

- Network & Infrastructure Protection - 100% of NSGs are configured to not expose all ports
- Data Protection - 100% of blob storage has encryption properly enabled
- Identity & Access Management - 100% of Kubernetes instances have RBAC enabled
- Logging & Monitoring - 100% of virtual machines have a VM Agent enabled

Negative Scan Findings

- Data Protection - There are instances of SQL database without the ability to restore configured
- Identity & Access Management - 2 Azure Web Apps are not registered with AD
- Logging & Monitoring - Activity Log alerts are not enabled for performance monitoring
- Network & Infrastructure Protection - 1 instance of a SQL server allows public access

Azure - Technical Assessment Overview



Summary

For the sampled account, there is a noted variance with how App Services and SQL Servers are configured. The variance of resource configuration may indicate a lack of controls enforcing standardization throughout the environment and forced adherence to secure baselines.



Observations

Technical Scan Finding

1	Two (2) out of 50 App Services were not using the latest version of PHP --- 3
2	Two (2) out of 50 App Services did not enforce the most recent version of HTTP --- 3
3	Two (2) out of 50 App Services did not require the use of client certificates to connect --- 4



Implication

- (1) Installing the latest version of PHP will reduce the security risk of missing security patches.
- (2) Outdated versions of HTTP have potential security vulnerabilities that are introduced to the environment
- (3) If incoming client certificates are enabled only an authenticated client with valid certificates can access the app.



Recommendations

- (1) Select the latest version of PHP for all PHP-based App Services
- (2) Enable HTTP 2.0 support in the general settings for all App Services
- (3) Enable incoming client certificate SSL setting for all App Services.

Azure - Identity & Access Management



Summary

Identity is managed centrally relying on the on premise Active Directory and SailPoint for the majority of administration and security controls. As these capabilities are then inherited to Azure, the majority of the risk is removed from the Azure environment. Opportunity does exist to further lock down the Azure IAM posture to prevent any local users from being created and leverage PAM solutions to secure highly sensitive credentials.

ID	Result	Observation	Importance to organization	Recommendation
IAM.1	Observation Noted - 4	Central Identity Management NiSource currently leverages the on-prem Active Directory (AD) instance to manage all users in Azure. The groups in the on-prem AD are then transferred into Azure to map the specific users to their roles within Azure. There is currently the ability to directly create users in Azure, however it is restricted to a single key administrator.	As NiSource's usage of Azure grows and additional administrators are added, these administrators may inherit the permissions to create additional users as well. This creates the risk of ad-hoc unmanaged users being created for the Azure environment.	- Implement technical safeguards (such as with Azure policy) to prevent the creation of new users within Azure AD by any user. - Scope future admin roles to remove permission sets regarding the management of users within Azure, which should only be managed by the connection to the on-prem instance.
IAM.2	Observation Noted - 4	Authentication to the Cloud Authentication at NiSource is currently managed by Active Directory and Ping Federate. MFA is required for all users who are accessing the Azure environment. Breakglass accounts are in the process of being configured within CyberArk.	Compromise of highly privileged accounts used for breakglass scenarios could lead to access to the entire environment and all resources within it.	Continue with the deployment of CyberArk to manage current highly privileged accounts and implement CyberArk for any highly privileged accounts created in the future.
IAM.3	No Observations	Role and Permission Management Permissions are managed using predefined Azure permission sets, which are mapped back to AD groups based on job function. Custom permission sets are stood up when needed to support specific services. Access reviews to these groups are automated via the Sailpoint implementation which is used with the on-premise AD instance.	-	-

Azure - Network & Infrastructure Protection



Summary

The network design in the Azure environment lacked segregation between environments as well as specific rules via network security groups. This model heavily relies on the existing Palo Alto implementation for all network protection and lacks security in layers. Introducing segregation between production and non-production environments helps to keep a logical boundary within the network topology and reduces the risk profile of the production applications.

ID	Result	Observation	Importance to organization	Recommendation
NIP.1	Observation Noted - 2	Network Design and Segregation The network design for NiSource's Azure environment utilizes a hub and spoke model with all traffic going through Palo Alto firewalls within the hub virtual network. However, there is no segregation between any of the networks within the Azure environment and they are all reachable to each other.	As more applications are developed in the Azure environment non-production and sandbox workloads will likely be deployed with less stringent security controls than a production workload. Due to the nature of the network configuration, lateral movement may be possible if there is an incident in a non-production environment, increasing the exposure of the production environment tremendously.	Configure network routing rules or network policies to segregate at a minimum, non-production and production workloads from each other.
NIP.2	Observation Noted - 3	Network Rules and Policies All network rules and policies are currently done with the Palo Alto firewalls located in the hub virtual network in the Azure environment. There are no NACLs or Network Security Groups(NSGs) being used for fine grained network policies within the Azure virtual networks themselves.	These use of specific network rules within NACLs and NSGs can be used to provide fine grained network restrictions within specific subnets or directly to specific Virtual Machines. This provides more control over the environment as various types of applications are deployed.	Configure baseline NACLs and NSGs which can be deployed to resources requiring complex connectivity requirements.
NIP.3	No Observations	Public Facing Protection The public facing application within the NiSource Azure subscription uses an Application Gateway with WAF policies configured to help prevent application layer attacks on it's public facing resources.	-	-

Azure - Logging & Monitoring



Summary

For the sampled Azure environment, logging and monitoring was fairly mature throughout, and all logs were being collected from various sources and sent to the Splunk instance if they were relevant to security. While performance logs were being collected, they are not utilized at this time leading to a lack in contextual performance metrics. The addition of performance logs can help give a larger picture around application health can help to give more clarity around the affect security incidents have to the environment.

ID	Result	Observation	Importance to organization	Recommendation
LM.1	No Observations	Log Sources All log sources within Azure are currently being collected, with security logs going to Splunk and performance logs being collected into Log Analytics.	-	-
LM.2	Observation Noted - 4	Log Centralization and Aggregation Logs are currently aggregated into two separate locations, with security logs going to Splunk and performance logs being collected into Log Analytics. Security logs are leveraged by the security teams to alert on any critical activity within the environment and performance logs are underutilized today.	Performance logs within the environment provide additional detail and context that may be helpful to understanding the full impact of security events, especially as it relates to the availability of applications.	Analyze available performance logs to discern which ones will provide additional insight into the applications. As the environment matures began to ingest these to help contextualize security alerts.
LM.3	No Observations	Alerting and Response Alerting and response for the Azure environment is currently handled by the centralized security team. They contact application owners for any remediation needed as the result of alerts. Additionally, they have standard incident response practices for the Azure environment which can be leveraged as needed.	-	-

Azure - Data Protection



Summary

The data protection posture in the Azure environment is fairly mature, with technical results showing the necessary functionality being enabled almost universally for all resources. Secure templates are being created for resources deployed into Azure to ensure that those security configurations are maintained as more resources are deployed. As the environment matures it may become necessary to begin to implement policy-as-code to enhance the guardrails around the secure templates, and to leverage posture management technology to a greater degree in order to prevent drift.

ID	Result	Observation	Importance to organization	Recommendation
DP.1	Observation Noted - 4	Securing Data at Rest The NiSource Azure environment uses standard terraform templates to ensure encryption at rest is being applied to all resources deployed into the environment. There is currently no utilization of Azure policies or monitoring of resource configurations to ensure there is no deviation from the standard templates.	While secure templates provide a secure baseline for engineering resources deploying to the cloud, there is a risk of these being bypassed without technical safeguards to block insecure configurations from being deployed.	- Implement Azure Policy or another policy-as-code mechanism to block and prevent insecure resources from being deployed. - Leverage existing CSPM technology to create continuous monitoring of resource configuration within the environment.
DP.2	Observation Noted - 4	Securing Data in Transit The existing applications deployed in the Azure environment do enforce encryption in-transit via various means on an application to application basis. There is no method to only allow encrypted connections in the environment today.	Without technical enforcement of encryption in transit, the responsibility falls onto developers and engineers to implement technology they may not be familiar with. In some cases this could lead to them bypassing standards designed to ensure security of critical data.	- Utilize technical means to enforce encryption as transit where possible. Potential methods include: - Utilizing Azure Policy to enforce requiring HTTPS on resources that support it - Limiting network connections to go over specific secure ports
DP.3	Observation Noted - 4	Asset Tagging and Classification Tagging within the NiSource Azure environment is primarily focused on tagging structured data with the type of data being stored there. There does not appear to be tagging in place for criticality of unstructured data today.	Ensuring proper tagging is in place for all resources within the Azure environment will assist in ensuring proper protections are in place based on the criticality and sensitivity of data across the environment. Even in instances where data is only being processed, proper protections need to be taken based off the data traversing the resources.	Define required tags based on data classification and modify Terraform templates to require tagging fields prior to deployment.

Azure - Disaster Recovery

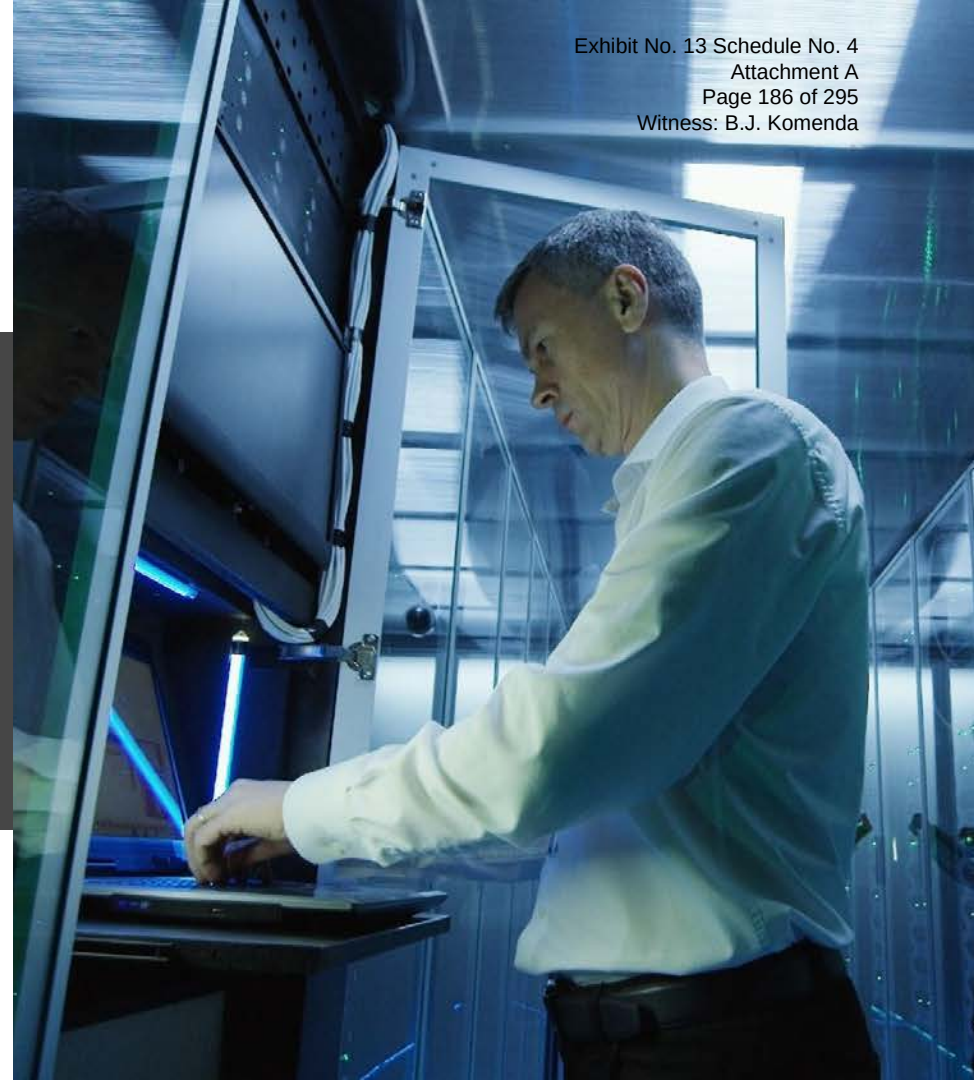


Summary

The Azure environment is currently not configured to be resilient and backups are limited. While it is currently a non-production environment, as the applications targeted for deployment will have resiliency and Disaster Recovery requirements building out this capability is critical to ensure the success of the applications in Azure. As the environment increases in complexity and replication to another region or the creation of a Disaster Recovery environment will also increase in complexity.

ID	Result	Observation	Importance to organization	Recommendation
DR.1	Observation Noted - 3	Backup Strategy Backups are not currently being leveraged within the Azure environment.	In the event of an error within the database, accidental deletion of data, or any other issue resulting in data loss, there is currently no means to recover this lost data via backups.	Critical databases and compute instances should be identified and both a backup strategy and backups be created using either Azure native backup capabilities or a third party technology.
DR.2	Observation Noted - 2	Resiliency Design NiSource's Azure environment has very few resources configured for high availability today, limited to just the Palo Alto firewalls and some applications items such as App Services and App Gateways. There is no additional region deployed at this time or disaster recovery capability but it has been noted that these items are on the roadmap for development as the Azure environment matures.	Additional regions and disaster recovery capabilities should be stood up ahead of any applications being launched to production in order to prevent downtimes in availability once the application is live. Additionally, the work required to enable these capabilities may increase tremendously once an application is live in the environment as changes become much more impactful to a live application.	Stand-up a second region with the required resources needed to support the level of disaster recovery dictated by the assigned criticality tier.
DR.3	No Observations	Application Criticality Management Application criticality is assigned on a scale used throughout NiSource of Gold, Silver, and Bronze. Each of these levels have different requirements regarding the applications availability and ability to recover from downtime. While there are currently no production applications in Azure, there are plans to conduct tests in the future as the incoming applications are within the Silver tier.	-	-

AWS Findings Summary



Risk Severity Rating

Remediation timelines, descriptions, and associated inherited risks are considered for each severity rating below:

Severity Level: 1



Description: Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company's reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

Severity Level: 2



Description: Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

- More than remote probability for damage to the Company's reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

Severity Level: 3



Description: Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

Severity Level: 4

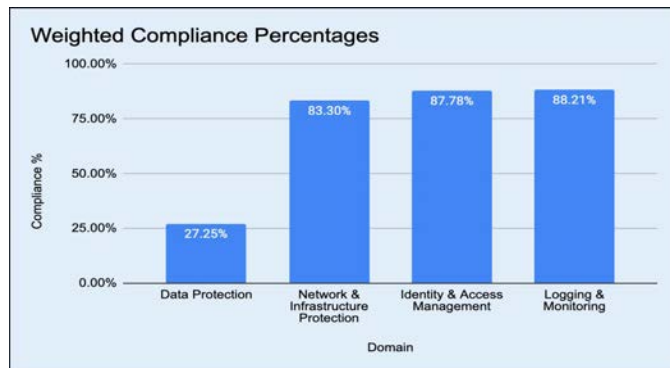


Description: Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited

Technical Results for AWS

The graphs below displays weighted compliance percentages for each of the domains assessed against AWS:



Note: The above graph displays overall weighted compliance % across the 4 domains assessed.

Key Takeaways

- ❖ Data Security has a much lower compliance score compared to the rest of the domains, primarily attributed to a large number of low severity findings
- ❖ While findings with higher ratings were limited to a few resources, they should be remediated immediately to improve security posture reduce risk exposure

Positive Scan Findings

- Data Protection - 100% of RDS instances and Redshift clusters have encryption at rest enabled
- Identity & Access Management - 100% of root accounts have MFA enabled
- Logging & Monitoring - CloudTrail is enabled for all accounts in all regions of the sampled environment
- Network & Infrastructure Protection - All Route53 domains have transfer lock set and are not expiring soon

Negative Scan Findings

- Data Protection - 43% of EBS volumes are unencrypted
- Identity & Access Management - 0% of Access Keys have been rotated in the last 180 days
- Logging & Monitoring - 0% of CloudTrail storage buckets have access logging enabled
- Network & Infrastructure Protection - There are 4 instances of network security groups with port 22 open to the public internet

AWS - Technical Findings



Summary

For the sampled accounts, the observations are primarily driven by a lack of security configurations for Cloudtrail logging buckets and inconsistency with networking rules. Cloudtrail logging buckets are crucial in the AWS environment as there is no integration with an on premise SIEM and they are the sole source of truth, while inconsistent networking rules could lead to oversights when securing the perimeter.



Observations

Technical Scan Finding	** Remediated	* Actively Remediating
1	Zero (0) accounts had access logging enabled on Cloudtrail buckets --- 2	
2	Four (4) of 104 Network Security Groups had port 22 for SSH exposed to the public --- 2	
3	One (1) of 104 Network Security Groups had all ports and protocols open to the public --- 2	
4	Zero (0) Cloudtrail logging buckets have a policy to prevent deletion without an MFA token --- 3	
5	Zero (0) of 68 Cloudtrail trails have encryption at rest enabled for logs --- 3	
6	50 of 117 EBS volumes are unencrypted at rest --- 3	
7	Nine (9) Access Keys haven't been rotated in over 180 days --- 3	
8	Four (4) Cloudtrail logging buckets are publicly accessible --- 3	
9	52 of 68 default Security Groups do not block all traffic by default --- 3	



Implication

- **(1)** Access logging enables the tracking of actions performed on buckets containing sensitive resources such as log files
- **(2)** More sensitive services such as SSH should be restricted to known IP addresses to prevent malicious access to privileged actions within systems.
- **(3)** Opening all ports and protocols exposes potentially unused services on an application and increases the attack surface
- **(4)** Requiring an MFA token helps to prevent accidental or malicious deletion of logs
- **(5)** Cloudtrail logs should be encrypted at rest to secure the sensitive data. Cloudtrail logs record all activity that occurs in the the account through API calls



Recommendations

- **(1)** Enable access logging on the CloudTrail bucket from the S3 console
- **(2)** Restrict access via TCP to port 22 to only known IP addresses and address ranges
- **(3)** Modify the security group to specify a specific port and protocol to allow.
- **(4)** Enable MFA delete on the CloudTrail bucket
- **(5)** Enable CloudTrail log encryption through the CloudTrail console or API

AWS - Technical Findings (cont.)



Summary

For the sampled accounts, the observations are primarily driven by a lack of security configurations for Cloudtrail logging buckets and inconsistency with networking rules. Cloudtrail logging buckets are crucial in the AWS environment as there is no integration with an on premise SIEM and they are the sole source of truth, while inconsistent networking rules could lead to oversights when securing the perimeter.



Observations

	Technical Scan Finding	** Remediated	* Actively Remediating
1	Zero (0) accounts had access logging enabled on Cloudtrail buckets --- 2		
2	Four (4) of 104 Network Security Groups had port 22 for SSH exposed to the public --- 2		
3	One (1) of 104 Network Security Groups had all ports and protocols open to the public --- 2		
4	Zero (0) Cloudtrail logging buckets have a policy to prevent deletion without an MFA token --- 3		
5	Zero (0) of 68 Cloudtrail trails have encryption at rest enabled for logs --- 3		
6	50 of 117 EBS volumes are unencrypted at rest --- 3		
7	Nine (9) Access Keys haven't been rotated in over 180 days --- 3		
8	Four (4) Cloudtrail logging buckets are publicly accessible --- 3		
9	52 of 68 default Security Groups do not block all traffic by default --- 3		



Implication

- **(6)** EBS volumes contain backups and potentially sensitive data stored on EC2 instances. Therefore it should be treated as such and encrypted.
- **(7)** Outdated keys could be potentially be compromised and unknowingly used to access the environment, best practice is to regularly rotate these keys.
- **(8)** CloudTrail logs may contain sensitive data regarding deployed resources and users, as such they should only be accessed by known and trusted users.
- **(9)** The default security group is often used for resources launched without a defined security group. For this reason, the default rules should be to block all traffic to prevent an accidental exposure.



Recommendations

- **(6)** Enable encryption for EBS volumes.
- **(7)** To rotate an access key, first create a new key, replace the key and secret throughout your app or scripts, then set the previous key to disabled. Once you ensure that no services are broken, then fully delete the old key.
- **(8)** Set the S3 bucket access policy for all CloudTrail buckets to only allow known users to access its files.
- **(9)** Update the rules for the default security group to deny all traffic by default.

AWS - Identity & Access Management



Summary

Identity is managed centrally relying on the on premise Active Directory and SailPoint for the majority of administration and security controls. As these capabilities are then inherited to AWS, the majority of the risk is removed from the AWS environment. Additionally, Service Control Policies are used to programatically prevent certain actions from being performed within the AWS environment helping to add another layer of enforcement.

ID	Result	Observation	Importance to organization	Recommendation
IAM.1	No Observations	Central Identity Management NiSource currently leverages the on-prem Active Directory(AD) instance to manage all users in AWS. The groups in the on-prem AD are then transferred into Azure to map the specific users to their roles within AWS Service Control Policies are further used to prevent IAM actions within AWS directly such as the creation of new users except by breakglass accounts..	-	-
IAM.2	No Observations	Authentication to the Cloud Authentication at NiSource is currently managed by Active Directory and Ping Federate. MFA is required for all users who are accessing the AWS environment. Breakglass accounts and root user accounts all require a Ubikey to access and login to.	-	-
IAM.3	No Observations	Role and Permission Management Permissions are managed using predefined AWS roles, which are mapped back to AD groups based on job function. The only custom roles are used for admins in the environment and tied specifically to their job function. Access reviews to these groups are automated via the Sailpoint implementation which is used with the on-premise AD instance.	-	-

AWS - Network & Infrastructure Protection



Summary

The network design in the AWS environment leverages a hub and spoke model, using the VPC structure initially created by Control Tower. Further fine grained control is put into place via specific subnets within VPCs segregating various parts of the applications. There is no access to the public internet within the AWS environment and all traffic goes through the on-premise environment and inherits the protections from the on-premise network stack.

ID	Result	Observation	Importance to organization	Recommendation
NIP.1	No Observations	Network Design and Segregation A hub and spoke model is used where possible, with a central networking/shared services VPC connected out. Additionally, there are separate VPCs for each app and environment deployed within AWS. Within each VPC there is additional segmentation with subnets to breakout the application and database layers.	-	-
NIP.2	No Observations	Network Rules and Policies Network Security Groups are used to fine grain access into the VPCs and Subnets. Additionally, all traffic to and from the internet must go through the on-premise firewall, which acts as the filtering point for all traffic in the environment.	-	-
NIP.3	N/A	Public Facing Protection There are no public facing applications in AWS. All network traffic must go through the on-premise environment where it passes through the on-premise firewalls, thereby inheriting these safeguards.	-	-

AWS - Logging & Monitoring



Summary

While some logging and monitoring was in place for the AWS environment, there was a lack of collection for certain critical logs, relying only on the log sources configured by AWS control tower. Additionally, these logs had not been integrated with the central log aggregation tool Splunk, making them less available to security teams. For alerting preconfigured CloudWatch alerts are relied on and due to the lack of Splunk integration the security team does not have the visibility or capability to create their own alerting mechanisms.

ID	Result	Observation	Importance to organization	Recommendation
LM.1	Observation Noted - 3	Log Sources CloudTrail is used and enabled by default via Control Tower which was used to help automate the setup. These CloudTrail logs along with some CloudWatch metrics are collected. There do not appear to be VPC Flow logs or any detailed configuration logs being collected within the environment at all.	The current log sources provide detail over specific actions taken which can be monitored via IAM calls within the AWS environment. Without VPC flow logs there will be no visibility into the actual network traffic taking place within the VPCs of the environment. Configuration logs help provide additional information into discrete changes made to resources in the environment and are needed to further contextualize risky actions.	• Enable VPC flow logs and ingest them into the preferred centralized logging solution • Either leverage existing CSPM technology to provide configuration data from the environment or enable AWS Config to provide logs and alerts relating to configuration
LM.2	Observation Noted - 3	Log Centralization and Aggregation The current AWS environment is sending CloudTrail logs to predefined buckets originally configured by Control Tower. These buckets however, are not forwarding the logs to Splunk or the security team with alerts being handled solely by CloudWatch events.	Without integration into the preferred log aggregation solution, security teams have tremendously decreased visibility into the AWS environment. Additionally, any investigative ability is hampered due to the fact they are unable to leverage a single platform to correlate various logs.	• Existing CloudTrail S3 buckets should be configured to forward their logs into the Splunk solution in order to centralize security logs from AWS
LM.3	Observation Noted - 2	Alerting and Response As the security team is not receiving an logs from the AWS environment they must rely on preconfigured CloudWatch alerts,	While CloudWatch logs are able to provide some alerting, they do not provide the customizability many security teams require to adopt all alerting best practices. Additionally, without the ability to monitor logs through a centralized solution response can be greatly affected.	• Analyze existing CloudWatch alerts and begin to move them over to the current alerting solution. Along with the ingestion of AWS logs to splunk, this will help streamline the Logging and Alerting process

AWS - Data Protection



Summary

The data protection posture in the AWS environment is fairly mature, with technical results showing the necessary functionality being enabled almost universally for all resources. Control Tower is being leveraged to create secure resources by design and when it is being used, many security configurations are created automatically. If the environment continues to grow it may become necessary to begin to implement policy-as-code to enhance the guardrails around resource creation, and to leverage posture management technology to a greater degree in order to prevent drift.

ID	Result	Observation	Importance to organization	Recommendation
DP.1	Observation Noted - 3	Securing Data at Rest NiSource's AWS environment leverages Control Tower for the setup of many resources within the AWS environment. This helps to enforce best practices such as enabling proper encryption across resources. There is however no means to enforce these settings via policy as code or a CSPM solution to prevent insecure configurations from being deployed manually.	While control tower helps to establish a secure baseline for resources deployed via this tool, there is a risk of controls being bypassed without technical safeguards to block insecure configurations from being deployed manually or configuration monitoring to identify them.	• Implement AWS Config or another policy-as-code mechanism to block and prevent insecure resources from being deployed. • Leverage existing CSPM technology to create continuous monitoring of resource configuration within the environment.
DP.2	Observation Noted - 3	Securing Data in Transit Encryption in transit is not enforced at all throughout the NiSource AWS environment as it is all internal traffic. As it is internal traffic HTTPS is not enforced until it is leaving the environment at the on premise firewalls, which leads to the public internet.	Without technical enforcement of encryption in transit, the responsibility falls onto developers and engineers to implement technology they may not be familiar with. In some cases this could lead to them bypassing standards designed to ensure security of critical data.	• Evaluate the type of data flowing throughout various connections and if it is decided that encryption in transit is needed enable it using the following methods: ◦ Utilizing AWS Config to enforce requiring HTTPS on resources that support it ◦ Limiting network connections to go over specific secure ports
DP.3	Observation Noted - 4	Asset Tagging and Classification Tagging within the NiSource environment does appear to be in place, however there is no technical enforcement to ensure specific tags and tag values are included for resources deployed.	Ensuring proper tagging is in place for all resources within the AWS environment will assist in ensuring proper protections are in place based on the criticality and sensitivity of data across the environment. Even in instances where data is only being processed, proper protections need to be taken based off the data traversing the resources.	• Implement AWS Config or another policy-as-code mechanism to block and prevent untagged resources from being deployed. • Leverage existing CSPM technology to create continuous monitoring of tagging configuration within the environment.

AWS - Disaster Recovery



Summary

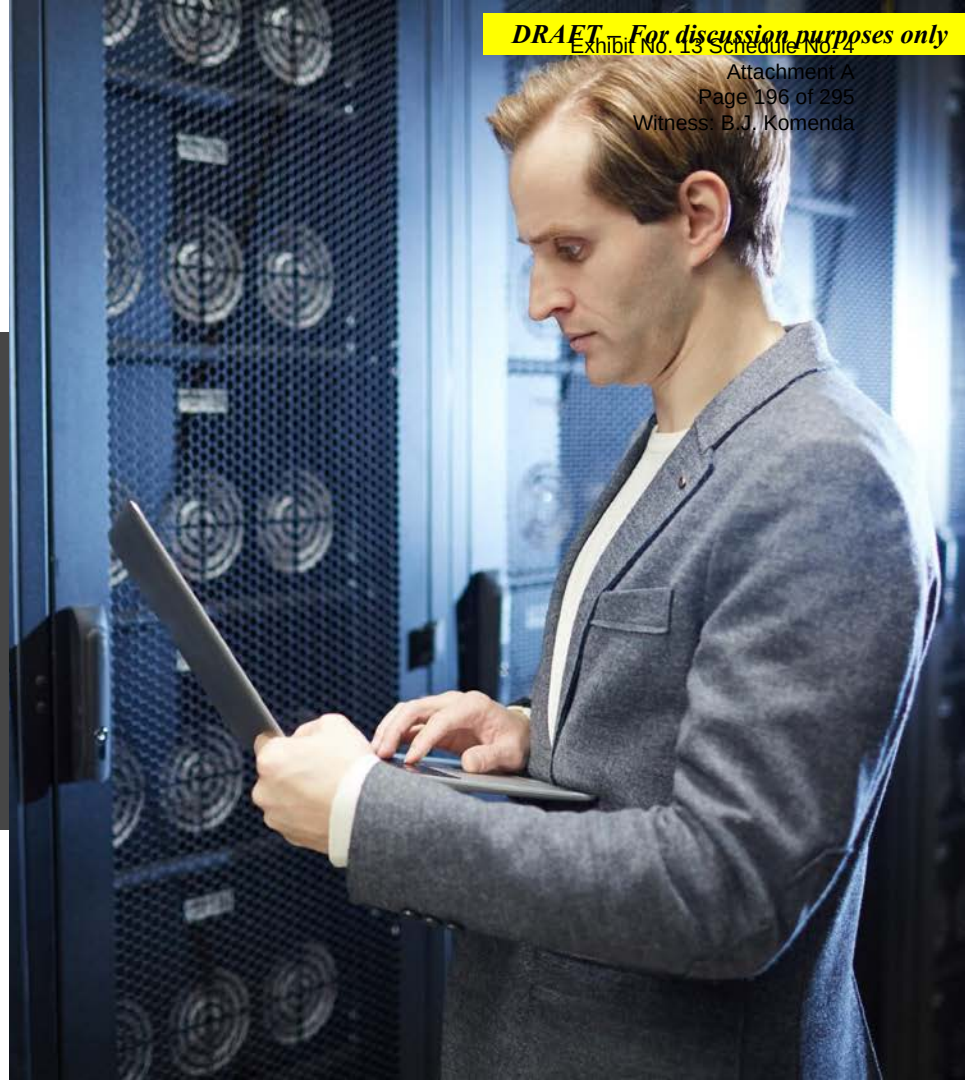
The AWS environment is currently configured to leverage a second region to store backups of in use databases which are backedup at regular intervals. While database backups are used, there is no resiliency in place for compute resources or ability to truly failover to a second region. All applications within the AWS environment are only rated to a Bronze criticality rating so these efforts may be outside of the scope that is required based on their business criticality.

ID	Result	Observation	Importance to organization	Recommendation
DR.1	No Observations	Backup Strategy For all relevant databases full backups are performed on a weekly basis and incremental backups are performed every day. These backups are stored in a backup vault in a second region (US East 1).	-	-
DR.2	Observation Noted - 4	Resiliency Design The applications deployed in the AWS environment are assigned the Bronze tier, which means the only requirements are that a best effort must be made when attempting to recover. In order to assist with this effort backups are stored in a separate region. While they do have a plan for recovery, there have been no formal tests since the environment was initially stood up. Additionally, while backups are in another region, there are no compute resources available across regions.	In the event of a region wide failure, while NiSource would maintain the ability to access the backed up data, they would have no ability to resume operations as compute resources rely on the original region. Additionally, as there have been no tests done to confirm the efficacy of recovery procedures. Adding AWS hosted applications to the scheduled recovery tests will assist in confirming the proper procedures are in place.	• Add regularly scheduled Disaster Recovery exercises for the AWS environment. • Evaluate the need for compute resources hosted in a recovery region to support full failover
DR.3	No Observations	Application Criticality Management Application criticality is assigned on a scale used throughout NiSource of Gold, Silver, and Bronze. Each of these levels have different requirements regarding the applications availability and ability to recover from downtime. The currently deployed applications in AWS are of tier Bronze. As they are only Bronze tier the only requirements are that a best effort be made to bring them back online. In practice this would translate to pulling in backups from the recovery region.	-	-

Appendix: Audit Observations Detailed List

DRAFT - For discussion purposes only
Exhibit No. 13 Schedule No. 4

Attachment A
Page 196 of 295
Witness: B.J. Komenda



Issue Overview

Result	Risk Rating 1	Risk Rating 2	Risk Rating 3	Risk Rating 4
Technical Results	0	3	8	128
Interview Based Results	0	3	6	8
Total	0	6	14	136

Azure Detailed Action Plans

CSP	ID	Source	Result	Issue	Management Action Plan	Responsible	Remediation Date
Azure	NIP.1	Control Workshop	Observation Noted - 2	Network Design and Segregation The network design for NiSource's Azure environment utilizes a hub and spoke model with all traffic going through Palo Alto firewalls within the hub virtual network. However, there is no segregation between any of the networks within the Azure environment and they are all reachable to each other. Risk As more applications are developed in the Azure environment non-production and sandbox workloads will likely be deployed with less stringent security controls than a production workload. Due to the nature of the network configuration, lateral movement may be possible if there is an incident in a non-production environment, increasing the exposure of the production environment tremendously.	IT Infrastructure Network management will complete the following actions: - Complete the knowledge transfer of the Azure tenant - Develop and execute a documented implementation plan to configure network routing rules and policies that will segregate non-production and production workloads	Jason Griffith, Director IT Infrastructure Network	The knowledge transfer of the Azure tenant was completed in February 2023. A plan to configure network routing rules and policies to segregate non-production and production workloads will be developed by May 2023; dates associated with specific action steps to be identified in the plan are to be determined.

Azure Detailed Action Plans

CSP	ID	Source	Result	Issue	Management Action Plan	Responsible	Remediation Date
Azure	DR.2	Control Workshop	Observation Noted - 2	Resiliency Design NiSource's Azure environment has very few resources configured for high availability today, limited to just the Palo Alto firewalls and some applications items such as App Services and App Gateways. There is no additional region deployed at this time or disaster recovery capability but it has been noted that these items are on the roadmap for development as the Azure environment matures. Risk Additional regions and disaster recovery capabilities should be stood up ahead of any applications being launched to production in order to prevent downtimes in availability once the application is live. Additionally, the work required to enable these capabilities may increase tremendously once an application is live in the environment as changes become much more impactful to a live application.	IT Infrastructure Cloud and Data Center management has completed the following actions: - Formally documented the decision to adopt a reference framework for deploying cloud first solutions in a single region and leverage cross region servers in time of need (based on application tier requirement) vs deployment of cross regional disaster recovery services as a warm site topology	Ishreth Sameem, Director IT Infrastructure Cloud & Data Center	The action plan was formally documented and approved as of February 2023.
Azure	NIP.2	Control Workshop	Observation Noted - 3	Network Rules and Policies All network rules and policies are currently done with the Palo Alto firewalls located in the hub virtual network in the Azure environment. There are no NACLs or Network Security Groups(NSGs) being used for fine grained network policies within the Azure virtual networks themselves. Risk These use of specific network rules within NACLs and NSGs can be used to provide fine grained network restrictions within specific subnets or directly to specific Virtual Machines. This provides more control over the environment as various types of applications are deployed.	IT Infrastructure Network management will complete the following actions: - Complete the knowledge transfer of the Azure tenant - Develop a documented implementation plan to configure baseline network access control lists and network security groups - Execute the configuration of baseline network access control lists and network security groups	Jason Griffith, Director IT Infrastructure Network	The knowledge transfer of the Azure tenant was completed in February 2023. A plan to configure baseline network access control lists and network security groups will be developed by May 2023; dates associated with specific action steps to be identified in the plan are to be determined.

Azure Detailed Action Plans

CSP	ID	Source	Result	Issue	Management Action Plan	Responsible	Remediation Date
Azure	DR.1	Control Workshop	Observation Noted - 3	Backup Strategy Backups are not currently being leveraged within the Azure environment. Risk In the event of an error within the database, accidental deletion of data, or any other issue resulting in data loss, there is currently no means to recover this lost data via backups.	IT Infrastructure Cloud and Data Center management will complete the following actions: - Formally document and approve the Azure Cloud Data Backup and Recovery Standards IT Infrastructure Cloud and Data Center management has completed the following actions: - Backup redundancy is in place leveraging Azure native backup capabilities	Ishreth Sameem, Director IT Infrastructure Cloud & Data Center	The action plan defined will be completed by March 2023.
Azure	DP.4	Technical Scan	Observation Noted - 3	Data Protection Two (2) out of 50 App Services were not using the latest version of PHP Risk Installing the latest version of PHP will reduce the security risk of missing security patches.	IT Infrastructure Cloud and Data Center management will complete the following actions: - Remove web development programming language (PHP) through the change management process as PHP is not being used	Ishreth Sameem, Director IT Infrastructure Cloud & Data Center	The action plan defined will be completed by March 2023.
Azure	NIP.4	Technical Scan	Observation Noted - 3	Network and Infrastructure Protection Two (2) out of 50 App Services did not enforce the most recent version of HTTP Risk Outdated versions of HTTP have potential security vulnerabilities that are introduced to the environment	IT Infrastructure Cloud and Data Center management will complete the following actions: - As part of the NS2 to SAP Rise project (SAP National Security Services), HTTP 2.0 will be enabled through the change management process	Ishreth Sameem, Director IT Infrastructure Cloud & Data Center	The action plan defined will be completed by June 2023.

AWS Detailed Action Plans

CSP	ID	Source	Result	Issue	Management Action Plan	Responsible	Remediation Date
AWS	LM.3	Control Workshop	Observation Noted - 2	Alerting and Response As the security team is not receiving an logs from the AWS environment they must rely on preconfigured CloudWatch alerts, Risk While CloudWatch logs are able to provide some alerting, they do not provide the customizability many security teams require to adopt all alerting best practices. Additionally, without the ability to monitor logs through a centralized solution response can be greatly affected.	Security management will complete the following actions: - Implement the integration Microsoft Defender for Cloud Applications with AWS that will enable logging and auditing in the AWS tenant	Jeremy Plante, Director Cybersecurity	The action plan defined will be completed by March 2023.
AWS	LM.4	Technical Scan	Observation Noted - 2	Logging Monitoring Zero (0) accounts had access logging enabled on Cloudtrail buckets Risk Access logging enables the tracking of actions performed on buckets containing sensitive resources such as log files	Security management will complete the following actions: - Implement the integration Microsoft Defender for Cloud Applications with AWS that will enable logging and auditing in the AWS tenant	Jeremy Plante, Director Cybersecurity	The action plan defined will be completed by March 2023.
AWS	NIP.4	Technical Scan	Observation Noted - 2	Network and Infrastructure Protection Four (4) of 104 Network Security Groups had port 22 for SSH exposed to the public Risk More sensitive services such as SSH should be restricted to known IP addresses to prevent malicious access to privileged actions within systems.	IT Infrastructure Cloud and Data Center management will complete the following actions: - In collaboration with Security and Network team, develop procedure documentation that will define approved ports and protocols for public domain - Implement corrections to remove public exposure for the ports and protocols exposed to the public	Ishreth Sameem, Director IT Infrastructure Cloud & Data Center	The procedure documentation will be developed by June 2023. The corrections will be implemented by September 2023.
AWS	NIP.5	Technical Scan	Observation Noted - 2	Network and Infrastructure Protection One (1) of 104 Network Security Groups had all ports and protocols open to the public Risk Opening all ports and protocols exposes potentially unused services on an application and increases the attack surface	IT Infrastructure Cloud and Data Center management will complete the following actions: - In collaboration with Security and Network team develop procedure documentation that will define approved ports and protocols for public domain - Implement corrections to remove public exposure for the ports and protocols exposed to the public	Ishreth Sameem, Director IT Infrastructure Cloud & Data Center	The procedure documentation will be developed by June 2023. The corrections will be implemented by September 2023.

AWS Detailed Action Plans

CSP	ID	Source	Result	Issue	Management Action Plan	Responsible	Remediation Date
AWS	LM.1	Control Workshop	Observation Noted - 3	Log Sources CloudTrail is used and enabled by default via Control Tower which was used to help automate the setup. These CloudTrail logs along with some CloudWatch metrics are collected. There do not appear to be VPC Flow logs or any detailed configuration logs being collected within the environment at all. Risk The current log sources provide detail over specific actions taken which can be monitored via IAM calls within the AWS environment. Without VPC flow logs there will be no visibility into the actual network traffic taking place within the VPCs of the environment. Configuration logs help provide additional information into discrete changes made to resources in the environment and are needed to further contextualize risky actions.	Security management will complete the following actions: - Implement the integration Microsoft Defender for Cloud Applications with AWS that will enable logging and auditing in the AWS tenant	Jeremy Plante, Director Cybersecurity	The action plan defined will be completed by March 2023.
AWS	LM.2	Control Workshop	Observation Noted - 3	Log Centralization and Aggregation The current AWS environment is sending CloudTrail logs to predefined buckets originally configured by Control Tower. These buckets however, are not forwarding the logs to Splunk or the security team with alerts being handled solely by CloudWatch events. Risk Without integration into the preferred log aggregation solution, security teams have tremendously decreased visibility into the AWS environment. Additionally, any investigative ability is hampered due to the fact they are unable to leverage a single platform to correlate various logs.	Security management will complete the following actions: - Implement the integration Microsoft Defender for Cloud Applications with AWS that will enable logging and auditing in the AWS tenant	Jeremy Plante, Director Cybersecurity	The action plan defined will be completed by March 2023.

AWS Detailed Action Plans

CSP	ID	Source	Result	Issue	Management Action Plan	Responsible	Remediation Date
AWS	DP.1	Control Workshop	Observation Noted - 3	Securing Data at Rest NiSource's AWS environment leverages Control Tower for the setup of many resources within the AWS environment. This helps to enforce best practices such as enabling proper encryption across resources. There is however no means to enforce these settings via policy as code or a CSPM solution to prevent insecure configurations from being deployed manually. Risk While control tower helps to establish a secure baseline for resources deployed via this tool, there is a risk of controls being bypassed without technical safeguards to block insecure configurations from being deployed manually or configuration monitoring to identify them.	IT Infrastructure Cloud and Data Center management will complete the following actions: - Implement standard operating procedures that will define policies to prevent insecure configurations from being deployed - Utilize Microsoft Defender for monitoring to identify when insecure configurations are deployed manually	Ishreth Sameem, Director IT Infrastructure Cloud & Data Center	The standard operating procedures will be developed by September 2023. The monitoring will be implemented by December 2023.
AWS	DP.2	Control Workshop	Observation Noted - 3	Securing Data in Transit Encryption in transit is not enforced at all throughout the NiSource AWS environment as it is all internal traffic. As it is internal traffic HTTPS is not enforced until it is leaving the environment at the on premise firewalls, which leads to the public internet. Risk Without technical enforcement of encryption in transit, the responsibility falls onto developers and engineers to implement technology they may not be familiar with. In some cases this could lead to them bypassing standards designed to ensure security of critical data.	IT Infrastructure Cloud and Data Center management will complete the following actions: - Evaluate type of internal data in Amazon Web Services environment, determine if encryption is required, and implement corrections if required	Ishreth Sameem, Director IT Infrastructure Cloud & Data Center	The action plan will be completed by September 2023.

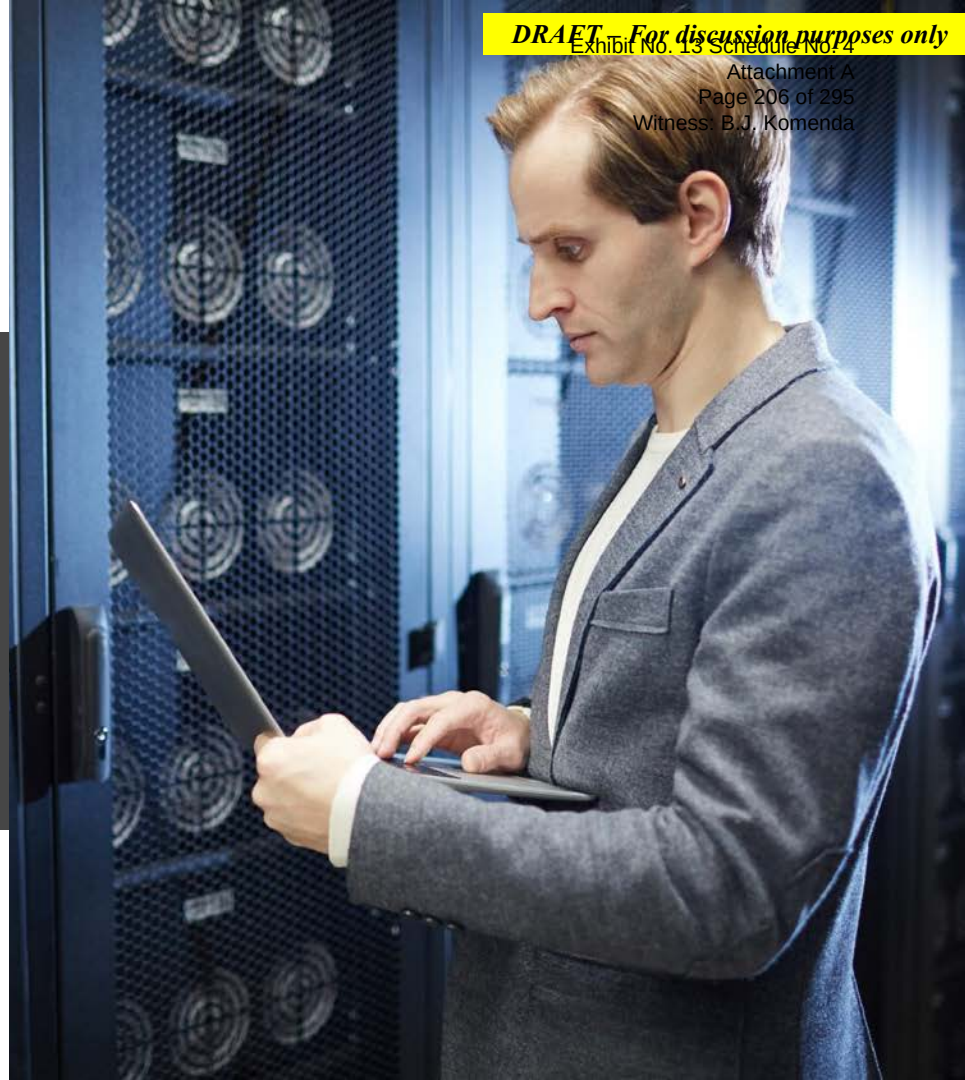
AWS Detailed Action Plans

CSP	ID	Source	Result	Issue	Management Action Plan	Responsible	Remediation Date
AWS	LM.5	Technical Scan	Observation Noted - 3	Logging and Monitoring Zero (0) Cloudtrail logging buckets have a policy to prevent deletion without an MFA token Risk Requiring an MFA token helps to prevent accidental or malicious deletion of logs	Security management will complete the following actions: - Implement the integration Microsoft Defender for Cloud Applications with AWS that will enable access logging in the AWS tenant	Jeremy Plante, Director Cybersecurity	The action plan will be completed by March 2023.
AWS	LM.6	Technical Scan	Observation Noted - 3	Logging and Monitoring Zero (0) of 68 Cloudtrail trails have encryption at rest enabled for logs Risk Cloudtrail logs should be encrypted at rest to secure the sensitive data. Cloudtrail logs record all activity that occurs in the the account through API calls	Security management will complete the following actions: - Implement the integration Microsoft Defender for Cloud Applications with AWS that will enable access logging in the AWS tenant	Jeremy Plante, Director Cybersecurity	The action plan will be completed by March 2023.
AWS	DP.4	Technical Scan	Observation Noted - 3	Data Protection 50 of 117 EBS volumes are unencrypted at rest Risk EBS volumes contain backups and potentially sensitive data stored on EC2 instances. Therefore it should be treated as such and encrypted.	IT Infrastructure Cloud and Data Center management will complete the following actions: - Formally document and approve AWS Cloud storage policies - Implement corrections to enable encryption for Amazon Block Store (EBS) volume devices through change management process	Ishreth Sameem, Director IT Infrastructure Cloud & Data Center	The policies will be developed by July 2023. The corrections will be implemented by September 2023.
AWS	DP.5	Technical Scan	Observation Noted - 3	Data Protection Nine (9) Access Keys haven't been rotated in over 180 days Risk Outdated keys could be potentially be compromised and unknowingly used to access the environment, best practice is to regularly rotate these keys.	IT Infrastructure Cloud and Data Center management will complete the following actions: - Create a standard operating procedures for access key rotation process - Develop and implement a plan to rotate the access keys	Ishreth Sameem, Director IT Infrastructure Cloud & Data Center	Development of procedure documentation will be completed by July of 2023. The access key rotation will be completed by September 2023.

AWS Detailed Action Plans

CSP	ID	Source	Result	Issue	Management Action Plan	Responsible	Remediation Date
AWS	LM.7	Technical Scan	Observation Noted - 3	Logging and Monitoring Four (4) Cloudtrail logging buckets are publicly accessible Risk CloudTrail logs may contain sensitive data regarding deployed resources and users, as such they should only be accessed by known and trusted users.	IT Infrastructure Cloud and Data Center management will complete the following actions: - Formally document and approve AWS Cloud storage policies - Implement corrections to limit public access to the Cloud Trail logging buckets	Ishreth Sameem, Director IT Infrastructure Cloud & Data Center	The storage policies will be developed and approved by July 2023. The corrections will be implemented by September 2023.
AWS	NIP.6	Technical Scan	Observation Noted - 3	Network and Infrastructure Protection 52 of 68 default Security Groups do not block all traffic by default Risk The default security group is often used for resources launched without a defined security group. For this reason, the default rules should be to block all traffic to prevent an accidental exposure.	IT Infrastructure Cloud and Data Center management will complete the following actions: - In collaboration with Security and Network team define procedure documentation that will define approved rule sets for security groups - Correct the default Security Groups that do not block all traffic by default	Ishreth Sameem, Director IT Infrastructure Cloud & Data Center	The procedure documentation will be developed by July 2023. The default Security Groups will be corrected by September 2023.

Thank You!





Internal Audit Department



We exist to deliver safe, reliable energy that drives value to our customers

Corrective Action Program Processes

Internal Audit Report

Distribution

Respondents:

Lauren Anderson

Beneficiaries:

Robert Heidorn
Paul Hunter

For Information:

Shawn Anderson
Melanie Berman
Melody Birmingham
Donald Brown
Kim Cuccia
William Jefferson
Lloyd Yates



Internal Audit Report

Background

The corrective action program (or CAP) is a foundational component of NiSource Inc.'s (NiSource or the Company) Safety Management System (SMS). The intent of CAP is to ensure that processes to evaluate identified issues are structured and documented and issue mitigation efforts are appropriately prioritized and monitored according to risk. The program was implemented for all NiSource gas companies as of August 2019 and incorporated the NiSource electric business in April 2021.

Any NiSource employee or contractor can submit an issue within the DevonWay application CAP module. The SMS team reviews submitted issues and follows an established process to facilitate risk evaluation and remediation plans. As of September 30, 2022, there were 2,216 reported issues outstanding. During the period of January 1, 2022, through September 30, 2022, there were 1,194 reported issues closed.

Audit Objective, Approach, and Coverage

The objective of this risk-based internal audit was to provide an independent evaluation of the adequacy, effectiveness, and efficiency of procedures and controls associated with the corrective action program. At the beginning of our audit, we completed a risk assessment, and we conducted detailed process assessments and sample-based transactional testing in higher-risk areas. The review period for this audit was January 2021 through September 2022.

During the audit, we specifically evaluated processes and controls related to:

- DevonWay CAP module user access and privileges
- DevonWay CAP module functionality specific to the assignment of unique reference numbers for submitted issues, identification and classification of required fields, and generation of automated email communications
- Adherence to CAP policies and procedures, specifically categorization of reported risks, approval levels, and closure processes
- Timeliness of issue evaluation and closure (i.e., cycle time appropriateness)
- Associated training requirements and activities
- Governance and reporting activities, including appropriate communication of key metrics

We did not evaluate issues submitted to the CAP module but transferred to be resolved through other processes outside of the program. Additionally, we did not evaluate subject matter expert decisions associated with risk scoring.

Internal Audit Finding Ratings

Internal Audit assigns ratings to audit findings based on the following scale (see the Internal Audit Finding Rating Scale in Appendix A):

"1" – Significant Improvement is Needed and Prompt Management Attention is Required

"2" – Improvement is Needed and Management Attention is Necessary

"3" – Some Improvement is Needed and Management Attention is Justified

"4" – Management Evaluation is Desirable

Internal Audit Conclusion and Summary of Observations

Prior to January 2023, employees responsible for executing corrective action program processes were largely decentralized and operated at a state level, resulting in inconsistent process execution and decisions. Centralization of the SMS activities under a single organizational structure should facilitate oversight and drive process consistency.

As a result of a continuous improvement effort initiated in the first quarter of 2022, the SMS Strategy and Execution team identified opportunities for improvement, including enhancements to causal analysis processes. Currently, the corrective action program only requires a formal causal analysis for cross bore or over pressurization issues. An events and near misses module of the DevonWay application is partially implemented, and could potentially be integrated with the

corrective action module to enable a more comprehensive analysis of identified issues and ensure proposed mitigation plans address both the symptoms and root cause of identified issues.

Overall, we noted that processes can be improved. We identified one finding associated with cycle time appropriateness where management's attention is required (Rating 1). We also noted one finding where management's attention is necessary (Rating 2). In addition, we observed some less-significant items that were discussed with management during the course of the audit.

A summary of audit findings rated "1" through "3" follows (see the Internal Audit Findings Matrix in Appendix B):

- 1) Corrective Action Program (CAP) Process Cycle Time Expectations (Rating 1)
Corrective action program policies and procedures define key process stages and the required steps in each stage, but cycle time guidelines and expectations are not defined. Additionally, monitoring procedures (specifically related to cycle time) are not formalized and executed to ensure appropriately paced progression through the CAP process stages and timely remediation of reported issues that is in alignment with risk.
- 2) CAP Risk Closure Process (Rating 2)
Current procedures for closing issues submitted in the DevonWay CAP module resulted in an issue, which is assessed as high risk, being closed prior to any operational risk reduction occurring. Specifically, the issue was closed when a mitigation action was added to a future workplan, versus when the mitigation action was completed. Closing issues based on an action being added to a future and mutable workplan, but prior to operationally reducing risk, decreases visibility to the issue and impairs remediation monitoring.

Management's Response

Management agrees with the findings noted during this audit and has provided action plans to address the risks identified. Management has taken immediate action to enhance the issues screening process and establish and track key performance indicators associated with program execution. Detailed action plans are included in Appendix B. The key mitigation steps will be completed by June 2023, with additional process refinements and associated training expected to be complete by January 2024.

Internal Audit Follow Up

Management has provided action plans for all findings with a rating of "1", "2", or "3". We have reviewed management's action plans and believe that the action plans will adequately address the findings identified in this audit. We will track the progress of resolution and will conduct follow-up testing for all rated "1" audit findings and a sample of rated "2" and rated "3" audit findings.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Report *****

"1" Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company's reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

"2" Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

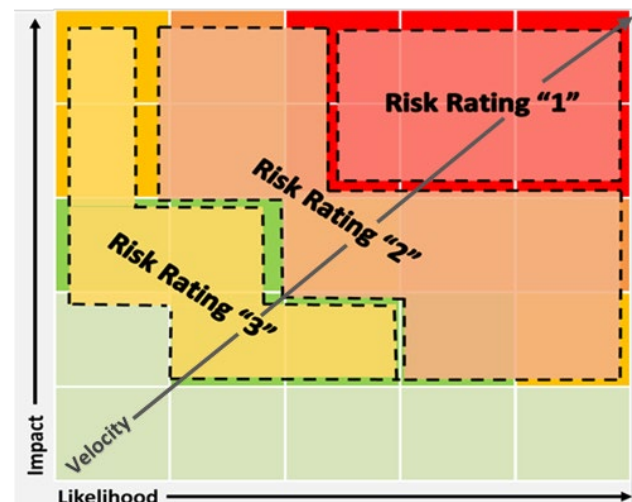
- More than remote probability for damage to the Company's reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

"3" Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

"4" – Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited



1) <u>Corrective Action Program (CAP) Cycle Time Expectations</u>	Rating: 1
<u>Risk:</u> Potential that delays in risk evaluation and remediation exposes the Company to increased operational, regulatory, and legal risk.	
<u>Observation:</u> While the corrective action program policies and procedures define key process stages and the required steps in each stage, cycle time guidelines and expectations are not defined. Additionally, monitoring procedures (specifically related to cycle time) are not formalized and executed to ensure appropriately paced progression through the CAP process stages and timely remediation of reported issues that is in alignment with risk. At the time of the audit, we identified that: • Thirty-two percent of reported issues outstanding were not risk rated, with 47 percent of that population relating to issues reported over a year prior; four issues were outstanding for over three years without being risk assessed • Sixty-four percent of the outstanding issues rated as high risk had not progressed past the action plan approval stage, and 48 percent of that population had been outstanding for over one year • For some reported issues, the approved remediation actions had occurred, but associated governance and administrative activities had not taken place to review and approve closure of the issue	<u>Management Action Plan:</u> The SMS Strategy and Execution team took immediate action to review the population of issues not risk rated, and we have decreased the percentage of items not risk rated from 32% to 11%. The team also began tracking cycle time metrics. In January 2022, the average days within the Screening workflow was 11 days. As of January 2023, the average days within the Screening workflow has been reduced to 4 days. Additionally, in January 2022, the average days in the SMS Lead Evaluation workflow was 76 days. As of January 2023, the average days within the SMS Lead Evaluation workflow has been reduced to 4 days. We have also completed the following actions as of March 1, 2023: • Established key performance indicators (KPIs) associated with cycle times, incorporate review of KPIs in governance venues (e.g., Risk Council) and distributed performance scorecards for use by Utilities Governance • Included CAP cycle time expectations in individual performance objectives for responsible employees • Assigned a designation of Adverse Condition or Continuous Improvement for an identified population of issues in the Screen, SMS Lead Evaluation, Issue Owner Evaluation, CAP Supervisor and Risk Review workflow status • Performed quality assurance reviews over the assignment of Adverse Condition or Continuous Improvement designation Additionally, the SMS Strategy and Execution team will complete the following: • Evaluate and process the remaining Adverse Condition issues without a risk ranking (June 2023) • Update CAP policies and procedures to incorporate newly established KPIs and process changes, including the addition of the quality control processes (August 2023)

	- Enhance KPI monitoring and review of performance metrics based on CAP process enhancements (November 2023) - Implement change management actions (e.g., training and outreach) to support understanding and consistent execution to support CAP KPIs (January 2024) <u>Responsible:</u> Lauren Anderson, Director SMS Strategy & Process <u>Resolution Date:</u> Target remediation dates are included for individual actions as indicated above.
<u>Criteria:</u> Target timeframes and performance metrics associated with the corrective action program support the achievement of business objectives and risk management strategies and are clearly defined, communicated, and monitored, specifically: 1) target timeframes and metrics are established for the key stages of the program; 2) responsible parties are adequately trained on performance expectations and targets and metrics are incorporated into individual performance objectives; 3) targets and metrics are consistently monitored and results are communicated to appropriate levels of management.	
2) <u>CAP Risk Closure Process</u>	
<u>Risk:</u> Potential an identified issue is not appropriately addressed or tracked and monitored resulting in the risk being realized.	
<u>Observation:</u> Current procedures for closing issues submitted in the DevonWay CAP module resulted in an issue, which is assessed as high risk, being closed prior to any operational risk reduction occurring. Specifically, the issue was closed when a mitigation action was added to a future workplan, versus when the mitigation action was completed. Closing issues based on an action being added to a future and mutable workplan, but prior to operationally reducing risk, decreases visibility to the issue and impairs remediation monitoring.	<u>Management Action Plan:</u> The SMS Strategy and Execution team will complete the following: - Enhance the CAP screening process to 1) identify continuous improvement opportunities and prioritize adverse conditions, 2) review and align the CAP risk model to the existing significance-based model and tie probabilistic Asset Knowledge Management risk models into the process as an input to prioritization and as an output to model updates (May 2023) - Clearly define and implement Functional Area Manager responsibilities and accountabilities within CAP to ensure clear action transition to business partners (May 2023) - Align new process with governance structure to ensure clear decision-making responsibilities and closure process (May 2023) - Develop and implement CAP quality assurance procedures which address proper closure (June 2023) - Update the DevonWay CAP module workflows to align with enhanced processes (November 2023)

- Execute change management activities to support implementation of process enhancements (January 2024)

Responsible:

Lauren Anderson, Director SMS Strategy & Process

Resolution Date:

Target remediation dates are included for individual actions as indicated above.

Criteria:

Policies and procedures are adequately designed, documented, and communicated to ensure the identified issues are not closed prior to being appropriately addressed; specifically: 1) processes are designed to ensure that issues are not closed until operational risk reduction occurs; 2) roles and responsibilities, including specific process execution objectives and requirements, are clearly defined; 3) responsible parties are adequately trained and understand how to properly execute the process; 4) quality assurance processes are designed and executed to identify and remediate exceptions to defined policy and procedures; and 5) open issues are monitored.

***** End of Report*****



Internal Audit Department



We exist to deliver safe, reliable energy that drives value to our customers

Gas Engineering Materials Quality Processes

Internal Audit Report

Distribution

Respondents:

Abigail Lauer
Connor McGrath
Crystal Miller

Beneficiaries:

Eric Belle
Sandra Brummitt
William Mojica
Jodi Santos
Steven Sylvester

Other Key Personnel:

Jake Upper

For Information:

Shawn Anderson
Melanie Berman
Melody Birmingham
Donald Brown
Kim Cuccia
William Jefferson
Michael Luhrs
Lloyd Yates



Internal Audit Report

Background

NiSource Inc. (NiSource or the Company) has six affiliated gas distribution companies that operate and maintain gas pipeline assets across six states. The Gas Standards and Compliance team is responsible for overseeing the material evaluation approval process to be followed when employees, contractors, vendors, or manufacturers request that materials, tools, or equipment (referred to herein as “materials”) be approved for use by NiSource companies.

Materials to be utilized for construction activities can be purchased through various processes and systems including directly with NiSource’s preferred materials vendor, MRC Global (MRC); through the applicable work management systems; through direct vendor invoicing through Ariba, the company’s invoice processing application; or by use of employee credit card with submission through Concur, the employee expense system.

Audit Objective, Approach, and Coverage

The objective of this risk-based internal audit was to provide an independent evaluation of the adequacy, effectiveness and efficiency of controls associated with the processes for approving new materials to be installed in gas pipeline facilities. We completed a risk assessment and conducted detailed process assessments and sample-based transactional testing in higher risk areas. The review period associated with the material approval requests evaluated during this audit was January 2021 through October 2022.

During the audit, we specifically evaluated:

- Policies and procedures that govern materials installed in gas pipeline facilities
- Processes for assessing/evaluating materials to potentially be installed in gas pipeline facilities
- Processes to maintain and communicate an approved materials listing
- Processes for approving manufacturers selected to source materials
- Controls established to prevent or detect the use of non-approved materials

We did not evaluate material receipt processes (including quality assessments upon delivery), materials traceability, materials recalls, or materials associated with non-pipeline components because these processes were or will be evaluated in other audits, or have relative lower risk.

Internal Audit Finding Ratings

We assign ratings to audit findings based on the following scale (see the Internal Audit Finding Rating Scale in Appendix A):

“1” – Significant Improvement is Needed and Prompt Management Attention is Required

“2” – Improvement is Needed and Management Attention is Necessary

“3” – Some Improvement is Needed and Management Attention is Justified

“4” – Management Evaluation is Desirable

Internal Audit Conclusion and Summary of Observations

Sustained collaboration and communication between the Gas Standards, Engineering, Supply Chain, Operations and Construction teams is imperative to ensure effective selection, approval, purchase, and installation of gas infrastructure materials. Purchasing activities and materials tracking processes are highly distributed, inconsistent, and executed via multiple channels using various information technology applications. NiSource is undergoing a technology transformation, including the introduction of a new work and asset management system, which is expected to standardize various operational practices. As part of this technology transformation, we recommend that management integrate and automate processes and controls related to gas materials purchasing and tracking, which will facilitate efficiency, consistency, and operational risk reduction.

Overall, we found that processes and controls related to the material selection and approval processes (as specified in the “Audit Objective, Approach, and Coverage” section of this report) should be improved. We identified one finding where management attention is necessary (Rating 2). We also identified two findings where management’s attention is justified (Rating 3). In addition, we observed some less-significant items that were discussed with management during the audit.

A summary of audit findings rated “1” through “3” follows (see the Internal Audit Findings Matrix in Appendix B):

- 1) Controls to Approve and Monitor the Use of Gas Infrastructure Materials (Rating 2)
Controls are insufficient to prevent unapproved gas infrastructure materials from being purchased and installed, and there are some instances where materials were installed without proper engineering evaluation and approval.
- 2) Vendor Governance Related to Material Identification Numbers Changes (Rating 3)
Requests to change materials master data within the Columbia Distribution Companies’ work management system are not timely processed, and the aging of materials master data change requests is not monitored.
- 3) Vendor Governance Related to Material and Manufacturer Quality Assurance Activities (Rating 3)
NiSource does not periodically validate MRC’s quality assurance activities or obtain and review evidence that MRC has undergone an independent assessment of their quality assurance program.

Management’s Response

Management agrees with the findings noted during this audit and has provided action plans that they developed to address the risks identified, with key actions targeted to be complete by December 2023. The remaining key mitigation steps will be completed by February 2024.

Internal Audit Follow Up

Management has provided action plans for all findings with a rating of “1”, “2”, or “3”. We have reviewed management’s action plans and believe that the action plans will adequately address the findings identified in this audit. We will track the progress of resolution and will conduct follow-up testing for all rated “1” audit findings and a sample of rated “2” and rated “3” audit findings.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Report *****

"1" Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company's reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

"2" Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

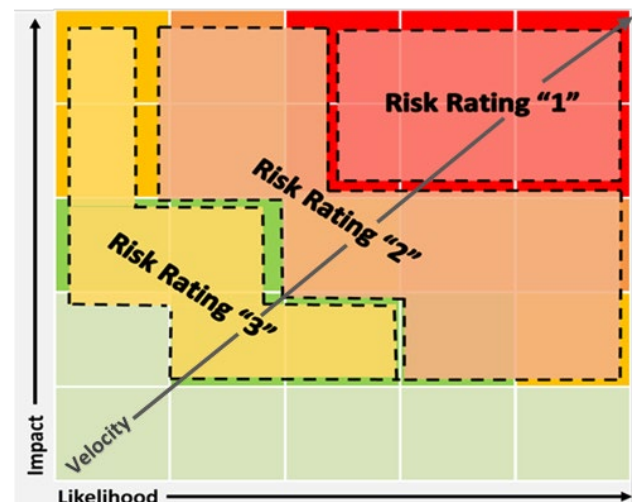
- More than remote probability for damage to the Company's reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

"3" Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

"4" – Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited



1) <u>Controls to Approve and Monitor the Use of Gas Infrastructure Materials</u>	Rating: 2
<u>Risk:</u> Potential that unapproved materials are purchased and installed in gas facilities, which could result in materials failures that cause negative operational outcomes.	
<u>Observation:</u> Engineering reviews and approves materials associated with design-capital job orders and the Gas Standards team issues gas standards that provide guidance regarding the required materials to be used in gas facilities. However, gas infrastructure materials can be purchased and installed in gas facilities without an appropriate engineering evaluation and authorization. Some field control activities, such as pre-in-service pressure tests and periodic leakage and corrosion surveys, improve the likelihood of detecting that installed materials are failing, but an unapproved material could fail after the facility is placed in service, resulting in negative operational outcomes. We evaluated a sample of materials purchased between January 2021 and October 2022 and identified instances where materials were purchased and installed without proper engineering evaluation and approval. Specifically, we noted: • A comprehensive catalog of approved materials is not codified and effectively communicated • While some guidance regarding gas facilities materials is referenced in standards and procedures, gas standards can be improved to ensure clarity regarding the specific types of materials requiring engineering evaluation • A master log of engineering evaluation requests is not maintained, request processes are inconsistent, and various formal and informal channels are utilized • Engineering materials evaluation results are not systematically documented, and existing documentation is inconsistently retained • A standard operating procedure is not defined to ensure gas infrastructure materials maintained within WMS and MAPPS available for purchase have been approved by Gas Standards or Engineering	<u>Management Action Plan:</u> The NiSource Gas Standards team, in conjunction with the Supply Chain team, will take the following actions to implement a materials approval process and associated change management controls, specifically: • Assess the risk of the identified unapproved materials installed and purchased and identify necessary remediation efforts, if necessary (May 2023) • Inform operations, construction and engineering departments of the expectation that Gas Standards or the Tool Team approve all materials for use and that effort is underway to formalize procedures and develop a singular Approved Material List (AML) for reference (May 2023) • Develop and publish a formal NiSource AML which includes materials used for gas-carrying facilities and materials that support system integrity (October 2023) • Develop and execute communications and a training plan associated with how the AML should be utilized (December 2023) • Develop a control to ensure that materials are verified against the AML prior to being added to materials masters/materials catalogs in the various systems used to purchase materials (December 2023) • Develop, publish and promulgate (in conjunction with Supply Chain) Gas Standards and associated procedures covering the materials request intake, vetting, and approval processes (procedures will also clarify that new materials shall not be used unless approved (October 2023) • Partner with Quality Management System team to consider potential audit steps or quality controls associated with materials that could be implemented during operational audits (Feb 2024) <u>Responsible:</u> Connor McGrath, Director Standards and Compliance

	<u>Resolution Date:</u> Refer to the target remediation dates for each action item listed above.
<u>Criteria:</u> Processes and controls have been established to ensure materials are properly evaluated and meet NiSource safety and performance standards prior to use, specifically: 1) types of materials requiring evaluation are identified; 2) roles and responsibilities associated with submitting requests, performing evaluations, and communicating results are clearly defined; 3) processes and supporting applications are established to retain evaluation documentation and timely update relevant reference materials; 4) impacted personnel are adequately trained to ensure process understanding; and 5) monitoring controls are established to identify exceptions in process execution.	
2) <u>Vendor Governance Related to Material Identification Numbers Changes</u>	Rating: 3
<u>Risk:</u> Potential for delayed purchasing activities resulting in operational inefficiencies or potential that personnel circumvent defined processes, which could increase the risk that unapproved materials are procured.	
<u>Observation:</u> Requests to change materials master data within the Columbia Distribution Companies' WMS are not timely processed, and the aging of materials master data change requests is not monitored. Changes to material master data within the work management systems, including creating and editing material identification numbers, are processed by Tata Consultancy Services (TCS), and NiSource's service level agreement with TCS defines the expected request response time as two business days. At the time of our review, 39 outstanding requests were pending, and 13 of the requests were aged more than 30 days, nine were aged more than 180 days, and 11 were outstanding for over a year.	<u>Management Action Plan:</u> Until action items from Finding #1 are executed, the Supply Chain team, in partnership with Gas Standards, is monitoring the population of outstanding materials master data change requests and the Supply Chain team will communicate acceptable escalation paths with TCS to ensure the third-party can timely resolve requests. Once the process enhancements from Finding #1 are finalized, the Supply Chain team will complete the following: • Enhance standard operating procedures specific to materials master data change processes executed by TCS to align with the updated processes and procedures developed as part of Finding #1 • Implement periodic performance monitoring processes over established SLAs for TCS • Communicate expectations to MRC associated with response times to TCS outreach and request that performance metric reporting be provided quarterly <u>Responsible:</u> Crystal Miller, Director Supply Chain Strategy & Analytics Abigail Lauer, Director Category Management <u>Resolution Date:</u> Outstanding materials data change requests are currently being monitored and escalation paths will be communicated by June 2023. The resolution dates of the remaining actions above are dependent upon implementation of the action items

outlined for Finding #1. Once the applicable action plans are complete, target remediation dates for the actions above will be determined.

Criteria:

Policies and procedures are adequately designed and executed to ensure third-party contractors performing work on behalf of the Company meet performance standards, specifically: 1) contract terms define measured metrics and potential outcomes of penalties for inadequate performance; 2) roles and responsibilities related to contractor governance are clearly defined and executed; 3) results of contractor assessments are reviewed timely to determine if additional action is required; and 4) submissions for variances are reviewed and approved timely.

3) Vendor Governance Related to Material and Manufacturer Quality Assurance Activities

Rating: 3

Risk:

Potential that materials produced do not meet technical specifications and requirements outlined by NiSource, and potential that utilization of sub-par material(s) results in negative operational outcomes.

Observation:

NiSource contracts with MRC to source materials from manufacturers on NiSource's behalf. Contract terms require MRC to maintain a Quality Assurance Program to ensure materials sourced by MRC meet performance specifications and quality standards, and contract terms specify that the results of audits performed by MRC over sub-tier suppliers are required to be provided to NiSource. However, NiSource does not periodically validate MRC's quality assurance activities or obtain and review evidence that MRC has undergone an independent assessment of their quality assurance program.

Management Action Plan:

In order for NiSource to evaluate the effectiveness of MRC's vendor quality assurance program, Supply Chain management will facilitate quarterly meetings with MRC and Gas Standards to review results of MRC's vendor quality assurance program.

In addition, Engineering Management will:

- Evaluate the adequacy of MRC's Quality Assurance Program or, obtain and review evidence of independent assessments engaged by MRC (e.g., ISO-9001 audits, SOC 2 Type 2)
- Validate the results presented during the quarterly meetings of MRC's vendor quality assurance program are in line with NiSource expectations

Responsible:

Abigail Lauer, Director Category Management
Eric Belle, VP Engineering & Standards

Resolution Date:

July 2023

Criteria:

NiSource has a defined quality assurance program agreement contained within the contract with MRC. MRC adheres to the contract requirements and NiSource independently reviews the results of MRC's quality assurance program.



Internal Audit Department



We exist to deliver safe, reliable energy that drives value to our customers

Data Center Operations Audit

Internal Audit Report

Distribution

Respondents:

Venkatesh Iyer
Kimberly Jones
Cecelia Largura
James Miller
Ishreth Sameem

Beneficiaries:

Waco Bankston
Percell Berry
Carla Donev
Kevin Johannsen
Andre Wright

For Information:

Shawn Anderson
Melanie Berman
Melody Birmingham
Donald Brown
Kim Cuccia
William Jefferson
Lloyd Yates



Internal Audit Report

Background

NiSource Inc. (NiSource or the Company) utilizes multiple data centers to deploy a geographically distributed service model to store, transfer, and access data. The data center environment consists of two corporate data centers in Hammond, Indiana and Columbus, Ohio that support approximately 340 applications utilized across the Company. The primary data center is in Hammond while the Columbus facility acts as a secondary location. Two co-location facilities located in Elk Grove, Illinois and Ashburn, Virginia, are managed by Equinix, Inc. and utilized for disaster recovery purposes if the NiSource-managed facilities are unable to maintain operations.

Audit Objective, Approach, and Coverage

The objective of this risk-based internal audit was to provide an independent evaluation of the adequacy, effectiveness and efficiency of controls associated with the data center environment for NiSource. At the beginning of our audit, we completed a risk assessment, and we conducted detailed process assessments and sample-based testing in higher risk areas. The services of Schneider Downs & Co, Inc. (Schneider Downs) were retained to perform this testing. Schneider Downs tested transactions related to the period between January 1, 2022 through December 31, 2022.

During the audit, we specifically evaluated processes and controls related to:

- Physical security and facility processes
- Backup, recovery, data replication, and high availability processes
- Business continuity and failover testing processes
- Environmental controls and emergency procedures
- Administration provisioning and monitoring
- Defining and monitoring vendor management
- Incident and problem management

We did not evaluate processes and controls related to the operational technology North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) data center operations and facilities.

Internal Audit Finding Ratings

Ratings are assigned to audit findings based on the following scale (see the Internal Audit Finding Rating Scale in Appendix A):

“1” – Significant Improvement is Needed and Prompt Management Attention is Required

“2” – Improvement is Needed and Management Attention is Necessary

“3” – Some Improvement is Needed and Management Attention is Justified

“4” – Management Evaluation is Desirable

Internal Audit Conclusion and Summary of Observations

The Information Technology (IT) organization is currently undergoing a technology transformation that includes activities related to data center operations. While this technology transformation will improve the Company's overall technology risk profile, IT management needs to remain focused on effectively managing change risk throughout the transformation lifecycle. NiSource engages third parties to perform key support activities related to data center operations, and vendor management and oversight controls are an important aspect of effectively managing risk related to data center operations. IT management should strive to ensure processes to validate and monitor the activities performed by third parties are robust and effective.

Overall, we found that processes and controls related to the data center operations activities (as specified in the "Audit Objective, Approach, and Coverage" section of this report) can be improved. We identified 2 findings requiring management's prompt attention (Rating 1). We also identified 1 finding where management's attention is necessary (Rating 2) and 1 finding where management's attention is justified (Rating 3). In addition, we observed some less-significant items that were discussed with management during the audit.

A summary of audit findings rated "1" through "3" follows (see the Internal Audit Findings Matrix in Appendix B):

- 1) Server Backup Controls (Rating 1)
Controls to ensure that backup schedules are appropriately modified when infrastructure changes occur are insufficient; as a result, backups were not performed for 33 servers supporting key applications governing data protection, data governance and retention, payroll management, gas availability reporting, customer cost reporting, regulatory reporting, and records management.
- 2) Physical Security Application Disaster Recovery and Business Continuity Controls (Rating 1)
Business continuity and disaster recovery activities for the applications controlling physical access to the data center and all other NiSource facilities are not managed per Company policy requirements, including the development of a business impact analysis, business continuity plan, and disaster recovery plan, and periodic testing as part of disaster recovery exercises.
- 3) Data Center Vendor Due Diligence Controls (Rating 2)
Vendor due diligence controls are insufficient related to some vendors utilized to support data center operations.
- 4) Physical Security Access Controls (Rating 3)
The practice to remove an employee's physical access to company facilities, including access to server rooms and data processing facilities, within 24 hours of termination has not been formalized and documented.

Management's Response

Management agrees with the findings noted during this audit and has provided action plans to address the risks identified. Detailed action plans are included in Appendix B. The key mitigation steps will be completed by August 2023.

Internal Audit Follow Up

Management has provided action plans for all findings with a rating of "1", "2", or "3". We have reviewed management's action plans and believe that the action plans will adequately address the findings identified in this audit. We will track the progress of resolution and will conduct follow-up testing for all rated "1" audit findings and a sample of rated "2" and rated "3" audit findings.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Report *****

"1" Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company's reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

"2" Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

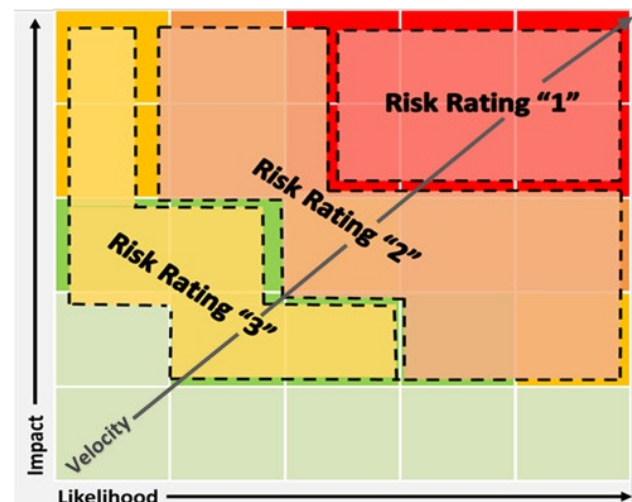
- More than remote probability for damage to the Company's reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

"3" Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited, and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

"4" – Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited



1) Server Backup Controls

Rating: 1

Risk:

Potential that data is exposed to malicious attacks and device failure resulting in loss of data and extended downtime of operations.

Observation:

The NiSource Inc. (NiSource or the Company) policy on data backups specifies server backup schedule requirements based on the classification and criticality of the information technology (IT) applications running on the servers. Server maintenance activities, including the addition of new servers to the appropriate backup software, are performed by Tata Consultancy Services (TCS). NiSource uses the Commvault backup and recovery platform to govern system backup and retention activities.

Controls to ensure that backup schedules are appropriately modified when infrastructure changes occur, including monitoring activities, are insufficient. During 2022, 33 servers added in the data center were not onboarded into Commvault, resulting in these servers not being backed up. These servers support 22 Tier 1 – Tier 4 applications (including applications governing data protection, data governance and retention, payroll management, gas availability reporting, customer cost reporting, regulatory reporting, and records management).

Management Action Plan:

IT Infrastructure management added the 33 servers to Commvault and required backups are now being executed. Additionally, TCS performed a full self-audit of all servers and the related backup schedules and identified additional servers that either were not backed up or were not backed up directly to Commvault. Required backups for these additional servers are now being executed as well.

IA recommends that IT Infrastructure management:

- Perform a root cause analysis to determine why the 33 servers identified as part of this audit, as well as the additional servers identified by TCS, were not included within the backup schedule
- Develop and execute a plan to ensure backup schedules are appropriately modified when infrastructure changes occur going forward based upon the results of the root cause analysis, including applicable changes to standard operating procedures provided to TCS to govern server maintenance activities, monitoring controls within NiSource to validate that all servers are being periodically backed up, and periodic self-audits performed by TCS

Responsible:

Ishreth Sameem, Director IT Infrastructure

Resolution Date:

The root cause analysis to determine why the servers were not included in the backup schedule will be completed by May 2023. A plan to address the completeness of backup schedules will be developed by June 2023; dates associated with specific action steps to be identified in the plan are to be determined.

Criteria:

Processes and controls are sufficient to ensure data is regularly backed up and available as needed and based upon risk.

2) **Physical Security Application Disaster Recovery and Business Continuity Controls**

Rating: 1

Risk:

Potential that the applications controlling physical access to the data centers and other NiSource facilities are unable to be recovered in the event of a disruption, resulting in unacceptable downtime or failure to restore the applications and access to facilities.

Observation:

The policy on IT business continuity and disaster recovery specifies requirements to ensure applications can be restored and business operations can continue in case of a service disruption, including the creation of a business risk assessment and business impact analysis for critical applications and the formalization and periodic testing of a business continuity and disaster recovery plan. However, business continuity and disaster recovery activities for the applications controlling physical access to the data center and all other NiSource facilities are not managed per the policy requirements, including the C•CURE ID Badging Solutions (C•CURE) badge reader system controlling physical access to the data center and all other NiSource facilities and the Immix Cloud (Immix) solution used for alerting; specifically:

- A formal business impact analysis has not been performed for C•CURE or Immix
- C•CURE has been assigned a criticality determination of Tier 1 for disaster recovery (i.e., critical and time sensitive recovery time required); while all Tier 1 applications should have a Gold service level agreement (SLA) designation for disaster recovery to ensure they are recovered within the appropriate amount of time, C•CURE has been assigned a Silver SLA tier within the ServiceNow configuration management database (CMDB)
- C•CURE and Immix are not included within the business continuity plan for Corporate Security
- A disaster recovery plan is not formally documented for C•CURE or Immix
- Neither application was included within recent disaster recovery exercises to ensure the applications can be recovered within the required recovery time objectives

Management Action Plan:

IT Applications management will work with Business Continuity management to perform the following:

- Conduct a formal business risk assessment and business impact analysis for C•CURE and Immix, in partnership with the service providers, in line with the requirements outlined within the IT Business Continuity and Disaster Recovery Policy
- Work with the Application Portfolio Management (APM) process owner to ensure that C•CURE and Immix are included in a formalized process to periodically review the risk assessments, business impact analyses, business continuity, and disaster recovery plans and update as appropriate
- Following the review of the current C•CURE and Immix applications and underlying infrastructure, develop an assessment to appropriately tier the applications and related infrastructure assets
- Based on the assessment and IT recommendation, implement change(s) to the current tiering of Application or Infrastructure within CMDB, if necessary
- Document a C•CURE and Immix-specific disaster recovery plan

Corporate Security management will perform the following:

- Update the Corporate Security Business Continuity Plan to include C•CURE and Immix

IT Infrastructure management will perform the following:

- Ensure that C•CURE and Immix are included in future disaster recovery exercises

Responsible:

Venkatesh Iyer, Director IT Applications
Cecelia Largura, Director Corporate Compliance & Business Continuity

James Miller, Director Corporate Security
Ishreth Sameem, Director IT Infrastructure

Resolution Date:

June 2023

Criteria:

Processes and controls are sufficient to ensure physical security applications can be restored in the event of a disruption.

3) Data Center Vendor Due Diligence Controls

Rating: 2

Risk:

Potential that third parties may expose organizational operations and/or data to unacceptable risk.

Observation:

NiSource's Cybersecurity third-party risk management policy requires that IT vendors are reviewed and periodically assessed based upon risk classification. The listing of service providers being utilized by the Federal Cyber Compliance team conducting the risk assessments did not include all technology vendors and, as a result, a vendor risk assessment has not been performed and the vendor risk classification has not been determined for seven of the 10 data center application and services vendors, including vendors governing storage, backup, and recovery services.

Additionally, processes and controls are not in place to periodically obtain the system and organization controls (SOC) reports for the two data center co-location vendors to review the operating effectiveness of their control environment as well as to review, implement and verify the effectiveness of NiSource's complimentary user entity controls (CUEC).

Management Action Plan:

Supply Chain has recently updated their onboarding process to support the Federal Cyber Assessment team by submitting all new technology supplier relationships for their review as part of the risk intake process.

IT Infrastructure management will perform the following:

- Develop a complete listing of all third-party vendors utilized in data center operations and provide the listing to the Federal Cyber Assessment team for use to perform their vendor risk assessment processes

Federal Cyber Assessment management will perform the following:

- Evaluate the listing provided by IT Infrastructure and perform vendor risk assessments for the identified vendors if warranted leveraging the risk intake process outlined within the Cybersecurity Third-Party Risk Management Procedure
- Formalize and implement a process to periodically obtain and review SOC reports for co-location vendors and implement and verify the effectiveness of identified CUECs as necessary

Responsible:

Ishreth Sameem, Director IT Infrastructure
Kimberly Jones, Director Federal Cybersecurity Compliance

Resolution Date:

The listing of vendors utilized within data center operations will be completed by June 2023. The review of identified vendors as warranted utilizing the risk intake

process, including the co-location vendors, will be completed by August 2023.

Criteria:

Processes and controls are sufficient to ensure vendors supporting data center operations are periodically reviewed and risk assessed to identify and manage vendor risk.

4) Physical Security Access Controls

Rating: 3

Risk:

Potential that unauthorized and/or inappropriate physical access to facilities, including data center assets, could result in security threats, asset misappropriation or damage, and negative impact to operations.

Observation:

While NiSource Corporate Security informally executes a practice to remove an employee's physical access to company facilities within 24 hours of termination, including access to server rooms and data processing facilities, this practice has not been formalized and documented within company policy. As a result, access to facilities, including data center access, is not always timely removed.

Management Action Plan:

Corporate Security management will perform the following:

- Formalize and document a process to review and remove physical access, including access to server rooms and data processing facilities, within 24 hours of termination and to obtain access badges at the time of termination within internal process documentation and the Corporate Security plans on the Company's intranet
- Train relevant associates on the updated requirements
- Implement a monitoring solution to identify instances where access has not been removed timely and/or badges have not been recovered

Additionally, Corporate Security, in collaboration with Human Resources (HR) and IT management, will consider if an IT solution can be implemented to automate the access removal process upon termination date.

Responsible:

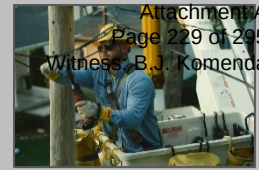
James Miller, Director Corporate Security

Resolution Date:

May 2023

Criteria:

Processes and controls are sufficient to ensure physical access to data center assets is restricted and monitored.



Internal Audit Department



We exist to deliver safe, reliable energy that drives value to our customers

Columbia Distribution Companies Customer Connect Processes

Internal Audit Report

Distribution

Respondents:

Eric Belle
Jeremy Plante
Patricia Potvin
Viji Jagabandhu

Beneficiaries:

Waco Bankston
Percell Berry
Michele Caddell
George Dice
Carla Donev
Kevin Johannsen
William Mojica
Matt O'Donnell
Jodi Santos
Gregory Skinner



For Information:

Shawn Anderson
Melanie Berman
Melody Birmingham
Donald Brown
Kim Cuccia
William Jefferson
Michael Luhrs
Lloyd Yates



Internal Audit Report

Background

NiSource, Inc. (NiSource or the Company) owns five distribution subsidiaries under the Columbia Gas brand (Columbia Gas Companies) that provide natural gas service to approximately 2.4 million customers in Ohio, Pennsylvania, Virginia, Kentucky, and Maryland. The New Business function, in collaboration with the Customer Care Center and Engineering teams, is responsible for profitably growing NiSource's customer base through new customer additions and added load. In 2022, over 16,700 opportunities for new customer additions and/or added load were assessed for the Columbia Companies, resulting in over 22,500 new meters being added to the distribution pipeline system.

Audit Objective, Approach, and Coverage

The objective of this risk-based internal audit was to provide an independent evaluation of the adequacy, effectiveness and efficiency of controls associated with the evaluation and approval processes to add new customers or customer load additions to our gas system. We completed a risk assessment and conducted detailed process assessments and sample-based transactional testing in higher risk areas. The review period associated with the customer connect processes evaluated during this audit was January 2021 through December 2022.

During the audit, we specifically evaluated processes and controls related to:

- New business assessment activities for new and existing customers
- New premise additions and linkage to customer information (including customer credit assessment, customer classification, and rate assignment activities)
- Reestablishment of service for existing premises
- Associated new business process technology controls

We did not evaluate NIPSCO gas and electric customer connect processes as this will be addressed as part of a separate audit.

Internal Audit Finding Ratings

We assign ratings to audit findings based on the following scale (see the Internal Audit Finding Rating Scale in Appendix A):

"1" – Significant Improvement is Needed and Prompt Management Attention is Required

"2" – Improvement is Needed and Management Attention is Necessary

"3" – Some Improvement is Needed and Management Attention is Justified

"4" – Management Evaluation is Desirable

Internal Audit Conclusion and Summary of Observations

While customer connect processes are generally well-functioning, diverse and ever-changing regulatory requirements across operating areas result in process inconsistencies. As such, management should focus on ensuring robust process documentation is created to capture key decision points and facilitate knowledge retention.

We found that Columbia Distribution customer connect processes and controls (as specified in the "Audit Objective, Approach, and Coverage" section of this report) were generally operating as intended. We identified two findings where management's attention is necessary (Rating 2) and one finding where management's attention is justified (Rating 3). In addition, we observed some less-significant items that were discussed with management during the audit.

A summary of audit findings rated "1" through "3" follows (see the Internal Audit Findings Matrix in Appendix B):

1) New Business Project Evaluation Processes (Rating 2)

An engineering assessment is required for new business projects that meet certain established criteria. A control to

validate/approve the determination of the necessity of an engineering assessment based on the established criteria is not formalized. As a result, required engineering assessments are not always conducted.

2) Customer Identity and Credit Verification Processes (Rating 2)

Interface controls that ensure requested credit information is returned from the third-party credit bureau and uploaded to the customer information system are not established and credit assessment information is missing for some customers, increasing the risk that the customer credit is not properly considered when determining required customer deposits.

3) SailPoint Application Onboarding Process (Rating 3)

User access was not thoroughly validated prior to the implementation of SailPoint, the identity and access management application, because the SailPoint application onboarding process does not include a step to review existing user access and remediate issues, resulting in some users having access to applications that is inconsistent with their current job responsibilities.

Management's Response

Management agrees with the findings noted during this audit and has provided six action plans that they developed to address the risks identified, with all actions targeted to be complete by July 2023.

Internal Audit Follow Up

Management has provided action plans for all findings with a rating of "1", "2", or "3". We have reviewed management's action plans and believe that the action plans will adequately address the findings identified in this audit. We will track the progress of resolution and will conduct follow-up testing for all rated "1" audit findings and a sample of rated "2" and rated "3" audit findings.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Report *****

"1" Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company's reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

"2" Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

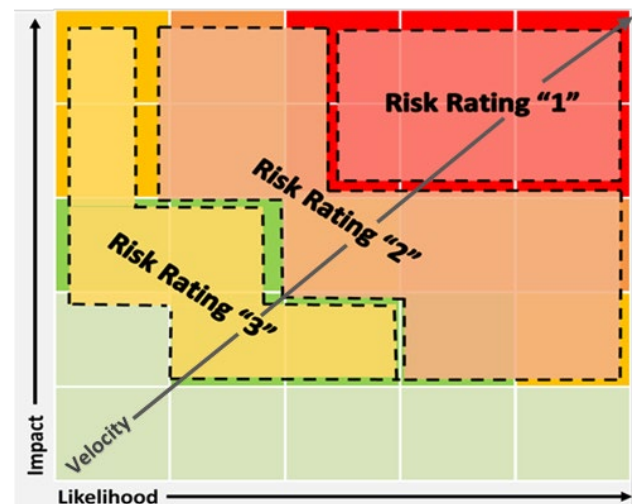
- More than remote probability for damage to the Company's reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

"3" Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

"4" – Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited



1) <u>New Business Project Evaluation Processes</u>	Rating: 2
<u>Risk:</u> Potential that pipeline reliability is negatively impacted related to new business projects.	
<u>Observation:</u> An engineering assessment is required for new business projects that meet certain established criteria. A control to validate/approve the determination of the necessity of an engineering assessment based on the established criteria is not formalized. As a result, required engineering assessments are not always conducted. We evaluated a sample of 26 new business projects closed between January 2021 and October 2022 and identified that three of 13 projects meeting the established criteria for an engineering assessment were constructed without being assessed by Engineering.	<u>Management Action Plan:</u> The New Business team, in collaboration with Engineering, will review evaluation criteria to ensure alignment with business needs and risk management objectives. If adjustments to criteria are necessary, training and reference materials will be updated and communicated. Additionally, the New Business team will complete the following: • Update established New Business quality assurance procedures (performed monthly) to assess engineering review determinations for a sample of projects and provide feedback and coaching to New Business personnel making determinations when necessary • Establish a process to periodically collaborate with Engineering and validate the accuracy of standard operating procedures, including evaluation criteria, and reinforce expectations and process requirements <u>Responsible:</u> Patricia Potvin, Director New Business Eric Belle, VP Engineering & Standards <u>Resolution Date:</u> July 2023
<u>Criteria:</u> Processes and controls are sufficient to ensure pipeline designs associated with customer opportunities are properly evaluated for service reliability, specifically: 1) roles and responsibilities are clearly defined and understood, 2) standard operating procedures and other reference materials are relevant and current, 3) personnel are appropriately trained, 4) validation and/or monitoring controls are formalized, and 3) feedback loops are sufficient to identify lack of adherence to requirements.	
2) <u>Customer Identity and Credit Verification Processes</u>	Rating: 2
<u>Risk:</u> Potential that the customer credit is not properly considered when determining required customer deposits, resulting in the Company taking on inappropriate credit risk.	
<u>Observation:</u> NiSource Inc. (NiSource or the Company) uses the services of Equifax Inc. (Equifax), a third-party credit bureau, to verify customer identity and determine customer deposit requirements. A data interface is established between the NiSource Columbia Gas Distribution	<u>Management Action Plan:</u> The DIS Application team noted that a control has been implemented to ensure Equifax uploads to the customer information system are timely and complete.

Companies' customer information system (DIS) and Equifax to facilitate this process; however, interface controls that ensure requested credit information is returned from Equifax and uploaded to DIS are not established and credit assessment information is missing for some customers.	<u>Responsible:</u> Viji Jagabandhu, Director Transformation Delivery <u>Resolution Date:</u> Management indicated that this action was completed in February 2023.
<u>Criteria:</u> Customer identity and credit is verified and utilized to determine any required customer security deposits prior to providing service, specifically: 1) roles and responsibilities are clearly defined and understood, 2) standard operating procedures are documented, relevant and current, 3) personnel are appropriately trained, 4) interfaces between Equifax and DIS are controlled and monitored.	
3) <u>SailPoint Application Onboarding Process</u>	
<u>Risk:</u> Potential that personnel who leave NiSource or who have changed roles inappropriately retain access to applications and improperly utilize available information or make unauthorized changes to application information.	
<u>Observation:</u> The Customer Relationship Management (CRM) application is utilized by the New Business team to store potential customers' information and project details. The New Load Tracking System (NLTS) is utilized by the New Business and Engineering teams to evaluate the serviceability of new and add load customers as well as obtain appropriate approvals of the capital project scope and design. While user access to the CRM and NLTS applications is currently managed using SailPoint IdentityIQ (SailPoint), which facilitates appropriate approval and review of user access, Sailpoint application onboarding processes did not require a formal review of existing user access prior to the Sailpoint implementation, and some people have access to the applications that is inconsistent with their current job responsibilities.	<u>Management Action Plan:</u> The New Business team has performed a review of CRM and NLTS users to ensure access is consistent with user job responsibilities. The NiSource Information Technology (IT) Identity and Access Management team will update SailPoint onboarding process to include a step to validate the appropriateness of application access. The Identity and Access Management and Technology Support teams will collaborate to develop a plan to ensure access reviews for non-Sarbanes-Oxley applications already onboarded into SailPoint are initiated and executed. <u>Responsible:</u> Patricia Potvin, Director New Business Jeremy Plante, Director IT Security Assignment for the third action item above is pending. <u>Resolution Date:</u> The first action item has been reported complete by management and remaining target remediation dates are pending.
<u>Criteria:</u> Controls are sufficient to ensure that access to data and application functions are appropriate and consistent with users' roles and responsibilities; specifically: 1) access to applications requires users to be authenticated to the Company's network using valid network credentials, 2) access requests are authorized by employees' direct supervisors and business data owners, 3) processes to terminate or change application access when users' roles and responsibilities change are formalized, and 4) access is periodically reviewed and validated to ensure granted access is appropriate in consideration of users' roles and responsibilities.	

4) **Customer Security Deposit Waiver Processes**

Rating: 4

Risk:

Potential that customer security deposits are inappropriately waived.

Observation:

Controls could be enhanced to ensure waivers of customer security deposits are in line with Company policy. We specifically noted all DIS users granted edit access can waive deposits or alter deposit amounts populated in DIS from Equifax without a secondary approval, and monitoring activities over waived deposits are not consistently executed or evidenced.

Management Action Plan:

As the risk associated with inappropriately waived security deposits is low, a management response is not requested; however, Internal Audit recommends that the Customer Operations and Customer Care Center teams collaborate to refine established monitoring processes to ensure a risk-based approach is applied to assess waived customer deposits. Additionally, as part of the NiSource IT transformation, we recommend that management consider the possibility of adjusting application access permissions within the future customer information system to limit users who can waive deposits and/or alter populated deposit amounts.

Criteria:

Waivers of customer security deposits are appropriate and in-line with Company policy, specifically: 1) standard operating procedures are documented, include waiver criteria, and related roles and responsibilities, 2) personnel are appropriately trained, and 3) monitoring procedures are sufficient to identify non-adherence to policy.



Internal Audit Department



We exist to deliver safe, reliable energy that drives value to our customers

Technology Capital Accounting

Internal Audit Report

Distribution

Respondents:

Christopher Cubenas
Kristen King
Matt O'Donnell

Beneficiaries:

Waco Bankston
Gunnar Gode

For Information:

Shawn Anderson
Melanie Berman
Melody Birmingham
Donald Brown
Kim Cuccia
William Jefferson
Lloyd Yates

Other Key Personnel:

Kevin Stanley



Internal Audit Report

Background

NiSource Inc. (NiSource or the Company) utilizes technology assets (including applications and the related hardware necessary to run and support the applications) to operate and support key business functions. As of December 31, 2022, NiSource maintained \$669.1 million in computer software and \$40.5 million in hardware assets with related software amortization of \$69.7 million and hardware depreciation of \$2.7 million. The Information Technology (IT) organization delivered 162 portfolios and projects in 2022 to add new technologies or update existing technology, with a total budget of \$176.6 million (\$156.0 capital and \$26.6 million operations and maintenance (O&M)).

Roles and responsibilities for technical accounting activities are distributed between the IT Project Management Office (PMO), which is responsible for governance, oversight, and compliance (including with accounting guidance) for IT projects and Fixed Asset Accounting, which is responsible for processing fixed asset transactions and maintaining asset balances within the fixed asset subledger (PowerPlant).

Audit Objective, Approach, and Coverage

The objective of this risk-based internal audit was to provide an independent evaluation of the adequacy, effectiveness, and efficiency of controls associated with technical capital accounting activities. We completed a risk assessment and conducted detailed process assessments and sample-based transactional testing in higher-risk areas. The review period associated with the transactions evaluated during this audit was September 2021 through August 2022.

During the audit, we specifically evaluated processes and controls related to:

- Technology asset capitalization policies and procedures, including adherence to United States Generally Accepted Accounting Principles (US GAAP) and Federal Energy Regulatory Commission (FERC) requirements
- Classification of technology expenditures as capital or O&M
- Classification of technology assets into asset category and related depreciation groups
- Completeness and accuracy of project cost tracking
- Depreciation expense calculation
- Associated accounting, including the completeness and accuracy of the data transfer from PowerPlant to PeopleSoft and fixed asset account reconciliations
- Review of technology expenditure information provided to Regulatory for inclusion in regulatory filings

Internal Audit Finding Ratings

We assign ratings to audit findings based on the following scale (see the Internal Audit Finding Rating Scale in Appendix A):

“1” – Significant Improvement is Needed and Prompt Management Attention is Required

“2” – Improvement is Needed and Management Attention is Necessary

“3” – Some Improvement is Needed and Management Attention is Justified

“4” – Management Evaluation is Desirable

Internal Audit Conclusion and Summary of Observations

The IT PMO and Accounting Research teams have partnered together to create robust guidance and training to drive accurate accounting of technology assets. Additionally, the NiSource Accounting team ensures that the Company's accounting guidance is aligned with external requirements while continually seeking to benchmark and implement best practices approaches. While accounting policies and procedures are robust, documentation pertaining to IT project spend, including accounting-related communications between the IT PMO and the Accounting Research team, can be enhanced. We recommend that management continue to pursue opportunities to improve activities that support consistent decisioning and IT project cost coding that is in accordance with accounting requirements.

Overall, we found that processes and controls related to the technology capital accounting activities (as specified in the "Audit Objective, Approach, and Coverage" section of this report) were generally operating as intended. We did, however, identify one finding where management's attention is necessary (Rating 2) and three findings where management's attention is justified (Rating 3). In addition, we observed some less-significant items that were discussed with management during the course of the audit.

A summary of audit findings rated "1" through "3" follows (see the Internal Audit Findings Matrix in Appendix B):

- 1) Capitalization of Software as a Service (SaaS) Licensing Costs (Rating 2)
Controls are not established to ensure the completeness and accuracy of the population of SaaS licenses recorded in the fixed assets subledger; as a result, we were unable to identify or quantify a complete listing of SaaS licenses to validate the effectiveness of processes to account for SaaS license costs.
- 2) Fixed Asset Accounting Risk and Controls Framework (Rating 3)
The current Sarbanes-Oxley (SOX) control framework and scope of testing performed should be enhanced to ensure the completeness and accuracy of fixed asset account balances within the Company's financial statements.
- 3) Software Renewal Fees Invoice Review Controls (Rating 3)
Documentation is inconsistently retained to validate the accuracy of accounting determinations utilized during the review of invoices for software renewal fees, including decisions to account for costs as either capital or expense.
- 4) IT Project Expenditure Review Controls (Rating 3)
Documentation evidencing that IT projects are reviewed and approved by the appropriate levels of management per Company policy requirements is inconsistently retained.

Management's Response

Management agrees with the findings noted during this audit and has provided action plans to address the risks identified. Detailed action plans are included in Appendix B. The key mitigation steps will be completed by February 2024.

Internal Audit Follow Up

Management has provided action plans for all findings with a rating of "1", "2", or "3". We have reviewed management's action plans and believe that the action plans will adequately address the findings identified in this audit. We will track the progress of resolution and will conduct follow-up testing for all rated "1" audit findings and a sample of rated "2" and rated "3" audit findings.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Report *****

"1" Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company's reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

"2" Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

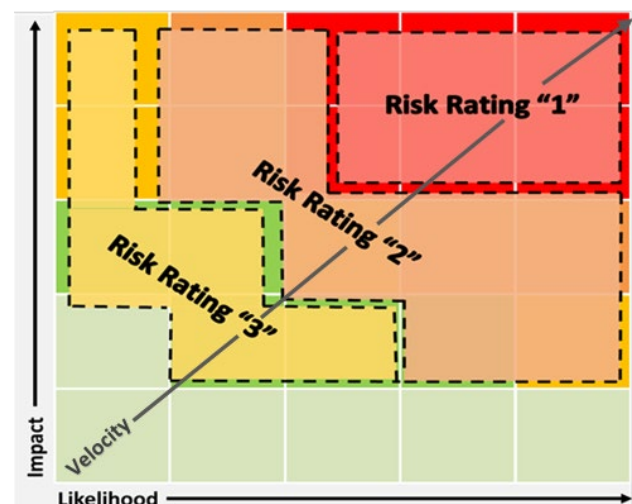
- More than remote probability for damage to the Company's reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

"3" Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

"4" – Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited



1) <u>Capitalization of Software as a Service (SaaS) Licensing Costs</u>	Rating: 2
<u>Risk:</u> Potential that expenditures associated with SaaS licenses are incorrectly capitalized, resulting in inaccurate financial and/or regulatory reporting.	
<u>Observation:</u> NiSource Inc. (NiSource or the Company) accounting policy allows for the capitalization of SaaS license expenditures if certain criteria are met, and a formal process is established for the Information Technology (IT) project management and Accounting Research teams to review and approve if SaaS licenses are eligible for capitalization. However, a control to ensure the completeness and accuracy of the population of capitalized SaaS licenses recorded in the fixed assets subledger (which is maintained in PowerPlant) is not established. A complete listing of SaaS licenses is not maintained and could not be identified or quantified. As a result, we were unable to validate the completeness and accuracy of SaaS licenses recorded as fixed assets.	<u>Management Action Plan:</u> IT Project Management Office (PMO) management will coordinate with the Accounting Research and Fixed Asset Accounting teams to develop a consolidated document to capture all known/documented applications (including SaaS and on-premise applications) and maintain a summary of the SaaS applications that were reviewed for potential capitalization with Accounting Research, including the application name, contract terms, license amount, date of Accounting Research review, and final capitalization determination. Contract terms, license amounts, date of Accounting Research review, and final capitalization determination will only be captured prospectively and will not be captured for all existing SaaS applications. Additionally, IT management will investigate if an IT solution can be leveraged to house the relevant SaaS capitalization information and documentation. <u>Responsible:</u> Matt O'Donnell, Senior Director Office of CIO Kristen King, Director Consolidations, External Reporting, Technical Accounting, & SOX Christopher Cubenas, Controller <u>Resolution Date:</u> May 2023
<u>Evaluation Criteria:</u> Controls and processes are sufficient to ensure that SaaS license related-expenditures are appropriately categorized as capital or O&M, specifically: 1) SaaS licenses are reviewed by IT to determine if they are eligible to be capitalized, 2) SaaS licenses that have been identified for capitalization are reviewed and approved by Accounting Research, and 3) Accounting Research's conclusion is documented and communicated to IT prior to capitalizing the related costs.	
2) <u>Fixed Asset Accounting Risk and Controls Framework</u>	Rating: 3
<u>Risk:</u> Potential that fixed asset misstatements are not timely identified and resolved leading to a financial reporting misstatement.	
<u>Observation:</u> The Sarbanes-Oxley (SOX) Compliance and the Fixed Asset Accounting teams are responsible for identifying risks and controls to ensure fixed asset balances are recorded completely and accurately in the financial statements. These controls are subject to annual testing by the SOX Compliance team. The current SOX control	<u>Management Action Plan:</u> Fixed Asset Accounting management will perform the following: Formalize a process to periodically review the CDC data transfer from PowerPlant to PeopleSoft to ensure

framework and scope of testing should be enhanced; specifically: - Fixed Asset Accounting activities rely upon automated system functionality to execute key processes to ensure asset balances are reflected completely and accurately in the financial statements; controls to validate the completeness and accuracy of the automated depreciation calculation in PowerPlant and the automated interface from PowerPlant to PeopleSoft for the Columbia Gas Distribution Companies (CDC) that transfers data related to fixed asset additions, retirements, depreciation expense, and overhead expenses are not performed or included in the SOX framework and testing procedures - The documented procedures for two SOX controls where the preparation is performed by Tata Consultancy Services (TCS) (processing of IT lease information provided by an external service provider into PowerPlant and processing of asset in-service dates) do not include a formalized and evidenced review step by Fixed Asset Accounting and review/approval of these controls is not performed - An existing SOX control to perform and review the monthly balancing of CDC in-service assets between the asset management system and PowerPlant is not being executed	all transactions were transmitted completely and accurately, including exception investigation and resolution - Formalize a process to periodically review the automated depreciation calculation functionality within Powerplant - Formalize processes to review the processing of both the IT lease information and asset in-service dates performed by TCS - Review the existing SOX control around the monthly balancing of CDC in-service assets between the asset management system and PowerPlant and update the control activities as appropriate based upon the necessary risk mitigation activities SOX Compliance management will perform the following: - Formalize the reviews of the automated depreciation calculation, data transfer between PowerPlant and PeopleSoft, the IT lease processing, and asset in-service date processing within the SOX control framework and quarterly testing process <u>Responsible:</u> Christopher Cubenas, Controller Kristen King, Director Consolidations, External Reporting, Technical Accounting, & SOX <u>Resolution Date:</u> The formalization and implementation of the processes outlined above related to the fixed asset controls will be completed by October 2023. The SOX Compliance team will partner with the Fixed Asset Accounting team to complete the action steps noted above by February 2024, including testing the operating effectiveness of the enhanced formalized processes.
<u>Evaluation Criteria:</u> Processes and controls are sufficient to ensure that SOX controls are properly identified, executed, and tested to address the risk of incomplete and/or inaccurate fixed asset balances within the financial statements; specifically: 1) risks and controls are formally identified and codified within the SOX control framework; 2) controls are timely executed and evidenced; 3) controls are tested; and 4) testing is properly documented, including formal sign-off by the process owner and a SOX Compliance team member in the SOX data management application.	
3) <u>Software Renewal Fees Invoice Review Controls</u>	
Rating: 3	
<u>Risk:</u> Potential that the lack of documentation supporting invoice review considerations, including capitalization decisions, makes the evaluation or confirmation of the process less efficient.	
<u>Observation:</u>	<u>Management Action Plan:</u>

While invoices related to technology asset spend are coded, reviewed, and approved for payment in accordance with the Company's policy on expenditure approvals and the IT capitalization requirements, these activities which are highly distributed across various project teams (including retention of documentation) are inconsistent. Also, documented policies do not require invoice review considerations and supporting documentation to be maintained. We requested documentation associated with a sample of 20 invoices to evaluate the accuracy of accounting determinations. Documentation supporting decisions to account for costs as either capital or O&M was unavailable for five (of 20) invoices for software renewal fees with a total value of approximately \$12.3 million.	IT Service management will formalize and implement a process to maintain supporting documentation for invoice review considerations for software renewal fees in a centralized location. <u>Responsible:</u> Matt O'Donnell, Senior Director Office of CIO <u>Resolution Date:</u> October 2023
<u>Evaluation Criteria:</u> Controls and processes are sufficient to ensure that expenses related to IT project spend are appropriately identified as capital or O&M spend, specifically: 1) IT project-related invoices are reviewed and approved for payment IT portfolio managers, 2) invoices are reviewed against the IT capitalization policy to determine whether costs should be capitalized or expensed, and 3) invoice charges are applied to the appropriate fixed asset balance(s) in PowerPlant by Fixed Asset Accounting.	
4) <u>IT Project Expenditure Review Controls</u>	
<u>Risk:</u> Potential that the lack of documentation supporting IT project budget considerations, including capitalization decisions, makes the evaluation or confirmation of the process less efficient.	
<u>Observation:</u> NiSource policy requires the review and approval of IT projects, including a breakout of the projected cost by capital vs. O&M expenditures, by identified levels of management based upon total project spend. Documentation evidencing that IT projects are reviewed and approved by the appropriate levels of management per the policy requirements is inconsistently retained.	<u>Management Action Plan:</u> IT PMO management has made a recent enhancement to the ServiceNow Project Portfolio Management (PPM) used to manage IT projects to capture the required capital authority approvals, in accordance with the Capital Governance Policy, as formal decisions within the system, including the necessary workflows and reporting. This enhancement provides a clear audit trail of the required approvals necessary and obtained for projects to move from the planning phase gate to the requirements phase gate. <u>Responsible:</u> Matt O'Donnell, Senior Director Office of CIO <u>Resolution Date:</u> Completed
<u>Evaluation Criteria:</u> Controls and processes are sufficient to ensure that IT project-specific spend has been identified and appropriately categorized as capital vs. O&M, specifically: 1) IT project budgets are determined and broken out by capital vs. O&M expenditures in accordance with the IT Capitalization Controls and processes are sufficient to ensure Policy requirements, 2) IT project spend over an established threshold is reviewed and approved by Accounting Research to ensure the capitalization vs. O&M determination is in accordance with Company policy, and 3) IT projects (including the budgeted expenditures) are reviewed and approved by the appropriate levels of management based upon identified spend.	

Rating: 3



Internal Audit Department



We exist to deliver safe, reliable energy that drives value to our customers

Technology Project Management Office Processes

Internal Audit Report

Distribution

Respondents:

Matt O'Donnell

Beneficiaries:

Waco Bankston

For Information:

Shawn Anderson
Melanie Berman
Melody Birmingham
Donald Brown
Kim Cuccia
William Jefferson
Lloyd Yates



Internal Audit Report

Background

NiSource Inc.'s (NiSource or the Company) Information Technology (IT) organization governs and delivers portfolios and projects with an intent to deliver required business solutions to support NiSource operations. In 2022, NiSource IT delivered 162 portfolios and projects budgeted at \$176.6 million (\$156.0 million capital and \$20.6 operations & maintenance (O&M) expense). In 2023, IT is planning to execute approximately 200 projects with a total budget of \$196.5 million (\$176.0 million capital and \$20.5 million O&M). To deliver these large-scale portfolios and projects, the IT Project Management Office (PMO) organization leverages a standardized project management framework and provides governance, oversight, and compliance for IT projects from demand to delivery.

Audit Objective, Approach, and Coverage

The objective of this risk-based internal audit was to provide an independent evaluation of the adequacy, effectiveness, and efficiency of controls associated with the IT PMO processes related to managing and monitoring large technology projects. At the beginning of our audit, we completed a risk assessment, and we conducted detailed process assessments and sample-based transactional testing in higher-risk areas. The review period for this audit was August 2022 through December 2022.

During the audit, we specifically evaluated processes and controls related to:

- IT Project management guidance, including roles and responsibilities and project phase gating requirements
- Project selection and approval processes
- Requirements management
- Testing and deployment controls adherence
- Budget and scheduling management and monitoring

We did not evaluate the ongoing Agile Transformation engagement. Additionally, we did not evaluate third party vendor management as this was reviewed as part of a separate audit of corporate vendor governance.

Internal Audit Finding Ratings

Internal Audit assigns ratings to audit findings based on the following scale (see the Internal Audit Finding Rating Scale in Appendix A):

"1" – Significant Improvement is Needed and Prompt Management Attention is Required

"2" – Improvement is Needed and Management Attention is Necessary

"3" – Some Improvement is Needed and Management Attention is Justified

"4" – Management Evaluation is Desirable

Internal Audit Conclusion and Summary of Observations

The IT PMO organization is focused on continuous improvement and has increased project oversight and rolled out a demand-to-delivery playbook that provides guidance to drive quality within and consistency across IT projects. While these initiatives have increased process maturity and facilitated consistency for IT projects, the organization can further improve monitoring and reporting to enable insights into process execution and compliance. We recommend that IT PMO management define and implement formal metrics and key stakeholder reporting to drive visibility into project performance, including budget and schedule adherence.

Overall, we found that processes and controls related to the areas tested (as specified in the “Audit Objective, Approach, and Coverage” section of this report) were generally operating as intended. We did, however, identify one finding where management’s attention is necessary (Rating 2) and one finding where management’s attention is justified (Rating 3). In addition, we observed some less-significant items that were discussed with management during the course of the audit.

A summary of audit findings rated “1” through “3” follows (see the Internal Audit Findings Matrix in Appendix B):

1) IT PMO Compliance Considerations Guidance (Rating 2)

IT project governance processes are insufficient to ensure that all compliance-related project deliverables are appropriately identified, executed, and approved and stakeholder feedback is adequately addressed during the demand and planning phases of the project lifecycle.

2) IT PMO Playbook Change Management (Rating 3)

Changes to the IT PMO playbook are not formally managed, approved, and communicated to key stakeholders, including guidance on how changes should be applied to existing and/or new projects.

Management’s Response

Management agrees with the findings noted during this audit and has provided action plans to address the risks identified. Detailed action plans are included in Appendix B. The key mitigation steps will be completed by July 2023.

Internal Audit Follow Up

Management has provided action plans for all findings with a rating of “1”, “2”, or “3”. We have reviewed management’s action plans and believe that the action plans will adequately address the findings identified in this audit. We will track the progress of resolution and will conduct follow-up testing for all rated “1” audit findings and a sample of rated “2” and rated “3” audit findings.

We would like to thank all personnel involved with this assessment for their cooperation and support throughout our review. If Internal Audit can be of further assistance, please contact us.

***** End of Internal Audit Report *****

"1" Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company's reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

"2" Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

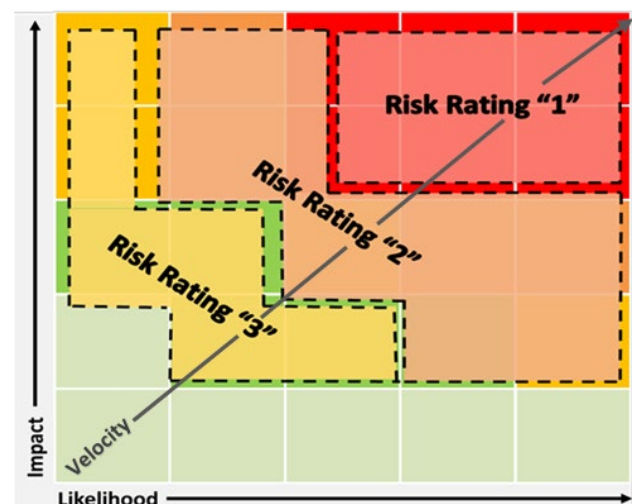
- More than remote probability for damage to the Company's reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

"3" Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited, and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

"4" – Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited

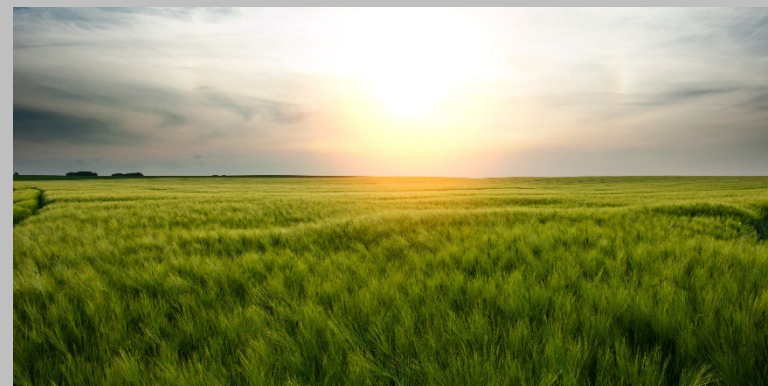


1) <u>Information Technology (IT) Project Management Office (PMO) Compliance Considerations Guidance</u>	Rating: 2
<u>Risk:</u> Potential that delivered technology solutions do not meet business, customer, and/or regulatory requirements leading to increased costs and business risk.	
<u>Observation:</u> The "IT Demand and Delivery Playbook" playbook (IT PMO playbook) serves as the prescriptive guidance for the execution of IT projects from demand to delivery and outlines key deliverables and roles and responsibilities throughout the project lifecycle. The IT PMO playbook guidance is insufficient to ensure required project deliverables have been identified and reviewed for the demand and planning project phases; specifically: • While a Sarbanes-Oxley (SOX) assessment is included within the planning requirements to ensure SOX-related control considerations are included within the project scoping requirements, the process is not formalized and signoff on the review is not required prior to completing planning • Additional compliance-related reviews are not required during planning, including the consideration of potential regulatory requirements • Within the project demand and planning phases, a formal review and approval of deliverables and phase completion are not required prior to moving forward with a project; as a result, stakeholder review comments are not always clearly addressed in project deliverables prior to completing the related project phase	<u>Management Action Plan:</u> IT PMO management will perform the following: • Create a formal deliverable within ServiceNow Project Portfolio Management (PPM) to document approval of all compliance considerations, including SOX, during the planning phase of an IT project • Formalize and define within the IT PMO playbook the required approvals for deliverables and phase completions for the demand and planning project phases <u>Responsible:</u> Matt O'Donnell, Senior Director Office of CIO <u>Resolution Date:</u> July 2023
<u>Criteria:</u> Guidance for IT project is sufficient to ensure each project phase has been completed and reviewed within the project lifecycle, specifically: 1) deliverables and required approvals for each phase of the project lifecycle are outlined and defined, 2) compliance considerations (including SOX) are included and required as part of the planning phase of IT projects, and 3) required phase completion reviews and approvals are outlined and defined.	
2) <u>IT PMO Playbook Change Management</u>	Rating: 3
<u>Risk:</u> Potential that IT project guidance is insufficient to drive effective project execution, resulting in delivered solutions that do not meet business and/or customer expectations.	
<u>Observation:</u> The IT PMO playbook is utilized by IT project teams to guide the execution of IT projects from demand to delivery for all three project delivery methods (agile, waterfall, and iterative). Changes to the IT PMO playbook are not formally managed, approved, and communicated to key stakeholders, including guidance on how changes should	<u>Management Action Plan:</u> IT PMO management has developed and implemented a formal process to document version control within the IT PMO Playbook. Additionally, IT PMO management will formalize a process to communicate IT PMO playbook changes

be applied to existing and/or new projects.	consistently throughout the IT organization, including outlining the applicability of changes to existing projects. <u>Responsible:</u> Matt O'Donnell, Senior Director Office of CIO <u>Resolution Date:</u> The formalization of process to document version control has been completed. The process to communicate IT PMO playbook changes will be implemented by July 2023.
<u>Criteria:</u> Controls and processes are sufficient to ensure IT PMO guidance is complete, accurate, and utilized by key stakeholders, specifically: 1) IT PMO guidance is periodically reviewed and updated as appropriate, 2) IT PMO guidance updates are formally managed and approved, and 3) changes to IT PMO guidance are formally communicated to key stakeholders.	
3) <u>IT Project Change Management</u>	
Rating: 4	
<u>Risk:</u> Potential that IT projects do not meet deliverables, time and/or cost expectations.	
<u>Observation:</u> Each IT project team is responsible for the management of the project to deliver the requested solution within the approved timeline and budget. While certain budget and high-level scheduling changes (e.g., project go-live dates) are managed through the formalized ServiceNow project change management (PCR) process, some project scope and schedule changes are not formally managed, reviewed, and approved (e.g., project phase and deliverable dates). Also, the PCR process guidance does not define criteria regarding change impact and priority and the application of these factors.	A management response is not requested; however, IT PMO management is actively monitoring the schedule management performance metrics being utilized by the Enterprise Project Management Office (EPMO) to measure phase gate and milestone performance for the Work and Asset Management (WAM) project to determine if similar tracking and approvals can be added to the current IT PMO process. Additionally, Internal Audit recommends that management update the PCR process guidance to define change impact and priority and how those should be applied based on the defined criteria.
<u>Criteria:</u> Controls and processes are sufficient to ensure that IT projects are managed, approved, and reviewed for budget and schedule adherence, specifically: 1) a process to review and approve project changes has been defined and formalized, 2) changes to project scoping, scheduling, and budgeting are reviewed and approved by appropriate levels of management per Company policy, 3) metrics to monitor budget and schedule adherence are defined, and 4) project metric reporting is reported to and reviewed by key stakeholders periodically.	



Internal Audit Department



We exist to deliver safe, reliable energy that drives value to our customers

NiSource Inc.

Customer Contact Center Technology Controls

Internal Audit Report

Distribution

Respondents:

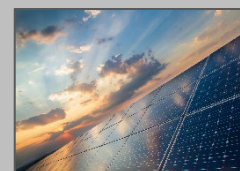
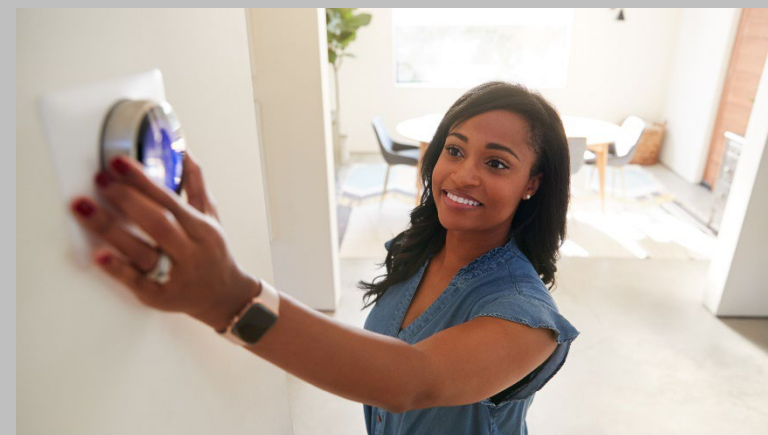
Heather Bauer
George Dice
Viji Jagabandhu
Cecelia Largura
Jeremy Plante
Ishreth Sameem

Beneficiaries:

Waco Bankston
Percell Berry
Carla Donev
Kevin Johannsen
Chuck Shafer
Andre Wright

For Information:

Shawn Anderson
Melanie Berman
Melody Birmingham
Donald Brown
Kim Cuccia
William Jefferson
Michael Luhrs
Lloyd Yates



Executive Summary

Key Insights	Key Background Information
- The Information Technology (IT) and Customer Contact Center teams are focused on enhancing the customer contact center technological ecosystem through the execution of projects that have the potential to improve employees’ and customers’ experience, including the 2022 Call Center Modernization (CCMOD) project and the ongoing Interactive Voice Recognition (IVR) refinement project - The coordination of multiple business and technology teams is required to ensure the accuracy and confidentiality of customer information and the reliability of key systems, but teams sometimes operate in silos and do not always effectively communicate, which could lead to misalignment resulting in issues that ultimately impacts customers	 Nearly 4 million customers  7.4 million calls received during 2022  Of which 1.3 million calls were handled by call center agents  7 key applications in the Customer Contact Center IT platform governing call routing, call waiting, call recordings, interactive voice response, and call center management
Count of Audit Findings by Scope Area	Audit Approach & Coverage
Configuration Management/Call Routing Prioritization 2 Data Security/Privacy 12 Disaster Recovery/Business Continuity Practices 1 System Access 2 Change Management Procedures No Findings Data Integrity No Findings Rating 1 Rating 2 Rating 3 Note: Less-significant observations were discussed with management during the audit.	We conducted a risk-based evaluation of the adequacy, effectiveness, and efficiency of procedural and systemic controls associated with NiSource’s customer contact center IT environment. We did not evaluate infrastructure-related controls or work performed as part of the IVR refinement project as the underlying processes are currently being reviewed and updated as part of ongoing projects. Additionally, we did not evaluate controls related to the external payment vendors as these were reviewed in a recent prior recent.

Summary of Findings

1) Customer Contact Center Business Continuity and Disaster Recovery Controls (Rating 1)

Business continuity and disaster recovery activities for the customer contact center applications are not managed per NiSource Inc. (NiSource or the Company) policy requirements, including the maintenance of current business impact analyses, business continuity plans, and development and periodic testing of a disaster recovery plan as part of disaster recovery exercises.

2) Third-Party Vendor Data Management Practices (Rating 1)

Processes and controls are insufficient to ensure customer information included within certain customer contact center application logs is adequately protected prior to transmission to external parties.

3) Data Classification and Protection for Customer Contact Center Applications (Rating 2)

Internal websites within the customer contact center environment are not consistently configured with secure and encrypted connections when transmitting customer-based information over the network.

4) Customer Contact Center Data Classification Processes (Rating 2)

Data classification has not been defined and reviewed for five applications within the customer contact center platform, including two applications containing personal identifiable information (PII).

5) Customer Contact Center Applications Access Management (Rating 2)

Processes and controls are insufficient to ensure that system access is appropriate based on assigned roles and responsibilities for the customer contact center applications.

6) Compliance with Password Policy Requirements (Rating 2)

Password standards required per Company policy are not enforced for two of the customer contact center applications.

7) Customer Contact Center Batch Job Processing Management (Rating 3)

Batch job processing failure alert email notifications are not configured for two customer contact center applications.

8) Customer Contact Center Call Capacity Monitoring (Rating 3)

Port capacity to handle customer calls through the Genesys application is not monitored.

"1" Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company's reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

"2" Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

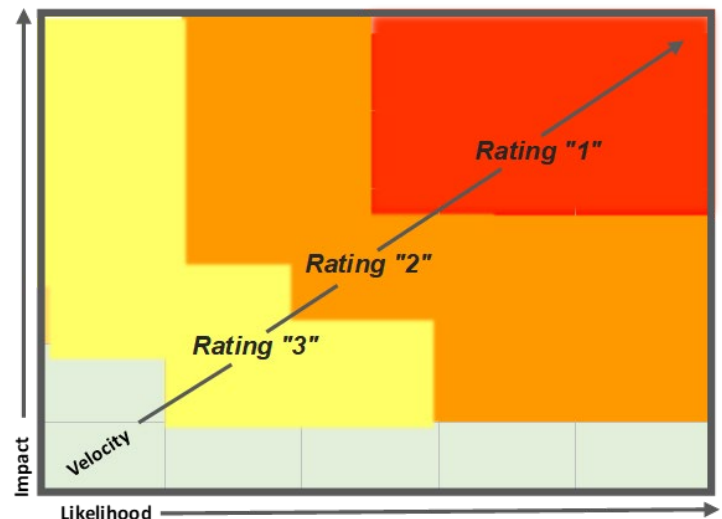
- More than remote probability for damage to the Company's reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

"3" Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

"4" Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited



1) **Customer Contact Center Business Continuity and Disaster Recovery Controls**

Rating: 1

Risk:

Potential that customer contact center applications are unable to be recovered in the event of a disruption, resulting in unacceptable downtime or failure to restore the applications.

Observation:

NiSource Inc.'s (NiSource or the Company) policy on information technology (IT) business continuity and disaster recovery outlines requirements to ensure applications can be restored and business operations can continue in case of a service disruption, including the creation of a business risk assessment and business impact analysis for critical applications and the formalization and periodic testing of a business continuity and disaster recovery plan. However, business continuity and disaster recovery activities for the customer contact center applications (including applications controlling customer voice and screen recordings, call routing, and customer support) are not managed per the policy requirements, specifically:

- While business impact analyses exist for the Northern Indiana Public Service Company (NIPSCO) and Columbia Gas (Smithfield) call centers, they have not been updated since 2019 and are not reflective of the current customer contact center environment, including applicable roles, applications, and application/process dependencies (e.g., analyses do not include all critical business, remote access, access management, and communications applications)
- Business continuity and contingency plans for the NIPSCO and Columbia Gas (Smithfield) call centers were last updated between 2017 and 2021 and are not reflective of the current risks within the customer contact center environment
- Customer contact center applications were not included within recent disaster recovery exercises to ensure the applications can be recovered within the required recovery time objectives (RTO)
- The Genesys Framework application has been assigned a criticality determination of Tier 1 for disaster recovery (i.e., critical and time sensitive recovery time required); while all Tier 1 applications should have a Gold service level agreement (SLA) designation for disaster recovery to ensure they are recovered within the appropriate amount of time, the Genesys Framework application has been assigned a Silver SLA tier within the ServiceNow Application Portfolio Management (APM)
- While the majority of the customer contact center platform applications have a disaster recovery criticality

Management Action Plan:

Customer Contact Center management has recently updated the business continuity plan for the Columbia Gas (Smithfield) call center. Additionally, Customer Contact Center management will work with Business Continuity management to perform the following:

- Update business continuity/contingency plan for the NIPSCO call center (August 2023)
- Update business impact analyses for the NIPSCO and Columbia Gas (Smithfield) call centers (October 2023)

Additionally, IT Applications management will work with Customer Contact Center and IT Infrastructure management to develop and execute a plan to update additional business continuity and disaster recovery documentation, including customer contact center application tiering information within APM, disaster recovery objectives and related deliverables, and documentation around the primary to secondary data center failover process, and to ensure the customer contact center applications are included in future disaster recovery exercises (the plan will be developed by October 2023; dates associated with specific action steps to be identified in the plan are to be determined).

Responsible:

Viji Jagabandhu, Director Transformation Delivery
George Dice, VP Customer Care Centers
Cecelia Largura, Director Corporate Compliance Business Continuity
Ishreth Sameem, Director IT Infrastructure

Resolution Date:

Refer to the target remediation dates for each action item listed above.

determination of Tier 1, the Nuance Insights, Nuance Web Admin Console, and Blackchair applications supporting the customer contact center environment have disaster recovery Tier 4 and 5 criticality determinations; additionally, these applications do not have defined RTOs and recovery point objectives (RPO) • While application restoration procedures (ARP) exist for four of the seven customer contact center applications, the ARPs do not identify dependencies on other applications (e.g., the data maintained within the NICE Voice and Screen Recording application is dependent upon the other customer contact center applications); additionally, the dependency upon VPN and Ping ID to access the applications through the NiSource network is not outlined • Disaster recovery runbooks outlining key disaster recovery steps are not defined for any of the customer contact center applications • While documentation exists regarding the primary to secondary data center failover procedures, it does not outline key and responsibilities, testing expectations and results, and required communications to key stakeholders	
<u>Evaluation Criteria:</u> Controls and processes are sufficient to ensure customer contact center applications can be restored in the event of a disruption; specifically: 1) business impact analyses and business continuity plans have been developed and contain all key applications and roles and responsibilities, and are periodically reviewed and updated; 2) business risk assessments have been developed and are periodically reviewed and approved; 3) disaster recovery criticality has been assessed and determined for all applications; 4) ARPs have been defined for all customer contact center applications; 5) disaster recovery runbooks have been developed and defined for all customer contact center applications; 6) failover procedures have been formally defined, along with testing procedures and results expectations, and shared with key stakeholders; 7) customer contact center applications are subject to periodic disaster recovery testing and testing results are shared with all relevant stakeholders.	
2) <u>Third-Party Vendor Data Management Practices</u>	Rating: 1
<u>Risk:</u> Potential that unprotected sensitive customer data is inappropriately disclosed resulting in increased costs related to remediation requirements and negative reputational impact.	
<u>Observation:</u> The customer contact center platform utilizes third-party applications to execute various activities that involve accessing sensitive customer account information. If issues with these applications are encountered, the application logs are provided to the vendor. Processes and controls are insufficient to ensure customer information included within some customer contact center application logs is adequately protected; specifically: • A process is not implemented to identify and mask and/or scramble sensitive customer information within	<u>Management Action Plan:</u> IT Applications management will perform the following: • Mask the sensitive customer information within the application logs (September 2023) • Work with Security and Legal Commercial management to develop and execute a plan to evaluate the need to share this data with external parties and determine what, if any, data protection, legal, and/or security procedures are required as a

the application logs that will be sent to vendors; as a result, personal information (PI) customer information within audit logs for the Genesys and Nuance applications including name, billing address, phone number, statement date and amount, customer account number, and customer ID is not masked or scrambled before the logs are sent to the vendors Genesys audit logs are transmitted outside of the United States to Europe, the Middle East, and Africa (EMEA) and Asia Pacific (APAC), but policy exception processes required per the Company's information classification and protection policy when data is shared outside of the country were not performed	result of the evaluation (A plan will be developed by October 2023; dates associated with specific action steps to be identified in the plan are to be determined) <u>Responsible:</u> Viji Jagabandhu, Director Transformation Delivery Jeremy Plante, Director IT Security Andre Wright, VP & Deputy General Counsel - Commercial <u>Resolution Date:</u> Refer to the target remediation dates for each action item listed above.
<u>Evaluation Criteria:</u> Controls and processes are sufficient to ensure that customer contact center audit log data is safeguarded and follows NiSource's data protection requirements; specifically: 1) the process to manage event and audit logs is formally defined and shared with stakeholders including third-party service providers; 2) audit logs are reviewed and categorized based on data classification requirements, including criticality or importance to the organization; 3) customer data within the logs is protected based on data classification levels prior to sharing with third parties; 4) third-party vendors follow the Company's data management and retention practices; 5) data transfer to third parties is reviewed and approval is received for all data transfers outside of the United States; and 6) reviews of vendor IT security programs are performed for vendors storing Company data outside of the United States.	
3) <u>Data Classification and Protection for Customer Contact Center Applications</u>	
<u>Risk:</u> Potential that data transmitted across an unsecured connection could be intercepted, resulting in the loss of customer data.	
<u>Observation:</u> NiSource's policy on data encryption standards specifies requirements to ensure that sensitive data is appropriately protected. Processes and controls to manage data security for the customer contact center applications are inadequate and do not comply with policy requirements and as a result, 31 of 44 internal websites within the customer contact center technological platform (including production, development, and quality assurance (QA)/test environments) are not configured with secure and encrypted Hypertext Transfer Protocol Secure (HTTPS) connections, including one website that is transmitting sensitive customer authentication data including customer account numbers, phone numbers, and partial social security numbers.	<u>Management Action Plan:</u> IT Applications management will embed policy-required encryption standards (e.g., HTTPS) for all identified customer contact center websites, including production, development, and QA/testing environments (i.e., Nuance WAC, NII, GAX, Genesys Admin, GCXI Standard Reports, GCXI Custom Reports, Pulse, WFM, Korbyt InView, Korbyt Admin, VHT Core, AudioCodes, and Blackchair). <u>Responsible:</u> Viji Jagabandhu, Director Transformation Delivery <u>Resolution Date:</u> October 2023
<u>Evaluation Criteria:</u> Controls and processes are sufficient to ensure that data is protected as appropriate, at rest or in-motion, across the customer contact center applications; specifically, that sensitive customer data within the applications is safeguarded and encrypted based upon the requirements for the assigned data classification.	

4) <u>Customer Contact Center Data Classification Processes</u>	Rating: 2
<u>Risk:</u> Potential that highly restricted or confidential customer data is inappropriately classified and safeguarded resulting in customer data loss and reputational impact to the organization.	
<u>Observation:</u> The Company's policy on information classification and protection specifies requirements to classify levels of data to determine how data should be secured and released to the public based upon sensitivity. However, data protection processes for the customer contact center applications are not managed per the policy requirements and as a result, data classification was not defined and reviewed within APM for five applications (Nuance Insights, Nuance Web Admin Console, NES 2.0, Virtual Hold Technology (VHT), and Blackchair); two of these applications (Nuance Insights and Nuance Web Admin Console) contain personal identifiable information (PII) data.	<u>Management Action Plan:</u> Customer Contact Center management will perform the following: • Work with the IT Applications team to evaluate the customer contact center applications against the Company's policy on information classification and protection and work with the IT Compliance team to update the data classification for each system within APM • Work with the IT Applications team to review the current application data usage against the data classification determinations and evaluate whether data usage is in compliance with data classification policy requirements <u>Responsible:</u> George Dice, VP Customer Care Centers Viji Jagabandhu, Director Transformation Delivery Heather Bauer, Director Compliance <u>Resolution Date:</u> January 2024
<u>Evaluation Criteria:</u> Controls and processes are sufficient to ensure that customer data is protected based on the sensitivity and applied classification; specifically, that application data has been reviewed, classified, and protected in accordance with the Company's policy on information classification and protection.	
5) <u>Customer Contact Center Applications Access Management</u>	Rating: 2
<u>Risk:</u> Potential that personnel who leave NiSource or who have changed roles inappropriately retain access to applications and improperly utilize available information or make unauthorized changes to application information.	
<u>Observation:</u> Processes and controls for user access to the customer contact center operations are insufficient to ensure that system access is appropriate based on users' assigned roles and responsibilities; specifically: • Some users have privileged access within NICE Voice and Screen Recording, Virtual Hold Technology (VHT) and Genesys Administrator that is inconsistent with their current job responsibilities • While user access to the customer contact center applications is currently managed using SailPoint	<u>Management Action Plan:</u> Identity and Access Management, IT Applications management, and Customer Contact Center management will work together to develop and execute a plan to formally define access management review processes, including the definition and documentation of system access roles and permissions for all customer contact center applications, the definition of review roles and responsibilities, frequency of review, and how instances of inappropriate access are managed. As previously noted within the 2023 Columbia Distribution Companies Customer Connect Processes audit report,

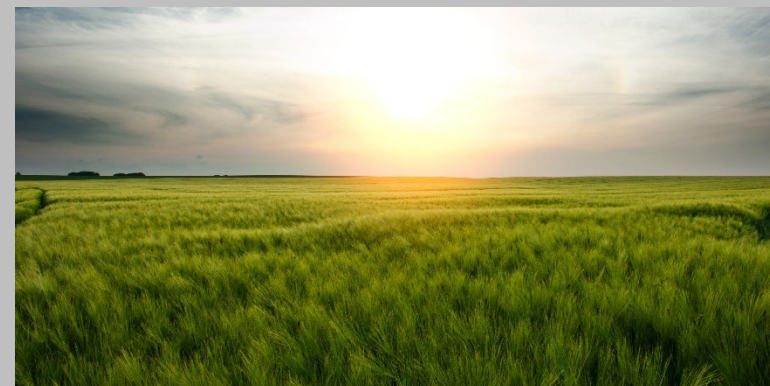
IdentityIQ (SailPoint), which facilitates appropriate approval and review of user access, the Sailpoint application onboarding processes did not require a formal review of existing user access prior to the Sailpoint implementation, and some employees have access to applications that is inconsistent with their current job responsibilities - System access roles configured within these applications are not formally defined and documented and therefore, the effectiveness of access reviews is reliant upon reviewers' understanding and knowledge of system roles, which could impair the reliability and consistency of these activities - While periodic user access reviews are performed for the customer contact center applications, the user access review process for these applications is currently assigned to reviewers who do not have the requisite knowledge and expertise to determine whether user access and roles are appropriate based upon job responsibilities for employees outside of the customer contact centers; for example, the access review for the NICE Voice and Screen Recording application contains over 1,400 users, while only 480 employees support the customer contact center environment	the NiSource Identity and Access Management team is working to update the SailPoint onboarding process to include a step to validate the appropriateness of application access. <u>Responsible:</u> Jeremy Plante, Director IT Security Viji Jagabandhu, Director Transformation Delivery George Dice, VP Customer Care Centers <u>Resolution Date:</u> A plan to formally define access management review processes will be developed by November 2023; dates associated with specific action steps to be identified in the plan are to be determined.
<u>Evaluation Criteria:</u> Controls and processes are sufficient to ensure that access to data and application functions are appropriate and consistent with users' roles and responsibilities; specifically: 1) application roles and responsibilities are defined and documented; 2) access requests are authorized by employees' direct supervisors and business data owners; 3) processes to terminate or change application access when users' roles and responsibilities change are formalized; 4) access is periodically reviewed and validated to ensure granted access is appropriate in consideration of users' current roles and responsibilities, including prior to loading application into SailPoint; and 5) inappropriate access as identified through periodic access reviews is removed in a timely manner.	
6) <u>Compliance with Password Policy Requirements</u>	
<u>Risk:</u> Potential that system availability is compromised and/or that data integrity is compromised, resulting in negative business consequences.	
<u>Observation:</u> NiSource's policy on identification and access management specifies password complexity requirements and requirements for individual passwords. Two of the applications utilized within the customer contact center platform (Genesys CX Insights and Virtual Hold Technology (VHT)) are maintained outside of the Company's single sign-on environment and as a result, password non-expiring and complexity rules are not enforced.	<u>Management Action Plan:</u> IT Applications management and IT Security management will work together to develop and execute a plan to enforce NiSource's password complexity requirements for Genesys CX Insights and VHT. Additionally, IT Applications management will look to leverage technology improvement opportunities within the upcoming Call Center as a Service (CCaaS) project to enhance password management for Genesys CX Insights and VHT to align with the Company's policy requirements.

	<u>Responsible:</u> Viji Jagabandhu, Director Transformation Delivery Jeremy Plante, Director IT Security <u>Resolution Date:</u> A plan to enforce NiSource's password complexity requirements for the two identified applications will be developed by October 2023; dates associated with specific action steps to be identified in the plan are to be determined.
<u>Evaluation Criteria:</u> Controls and processes are sufficient to ensure passwords for the information within the customer contact center applications are monitored to ensure data integrity; specifically: 1) temporary or default passwords are changed subsequent to installation in the Company's environment; 2) password complexity is enforced in line with Company policy; 3) password expiration rules are established and enforced; 4) account lockout after unsuccessful login attempts has been defined and enforced; 5) password encryption, storage, logging, and monitoring are enabled and evidence of inappropriate access is reviewed.	
7) <u>Customer Contact Center Batch Job Processing Management</u>	
Rating: 3	
<u>Risk:</u> Potential that the failure of key customer contact center batch processes will result in application interruptions and an inability to service customer requests.	
<u>Observation:</u> Batch processing is used to execute a large number of transactions concurrently and within the customer contact center environment, 45 batch jobs are used for backups, scheduling, and database clean-ups. While these jobs run without human intervention, and standard alerts are generated when a job fails, email alert notifications have not been configured for Genesys CX Insights and VHT. Additionally, policies and procedures have not been documented to address management of batch job failures, recovery strategies, and how to perform root cause analysis to address a potential issue.	<u>Management Action Plan:</u> IT Applications management will perform the following: - Establish email alert notifications for Genesys CX Insights and VHT for when batch jobs fail - Formalize batch job processes, specifically job failure process, root cause analysis process, and recovery strategy and distribute the document to relevant employees <u>Responsible:</u> Viji Jagabandhu, Director Transformation Delivery <u>Resolution Date:</u> October 2023
<u>Evaluation Criteria:</u> Controls and processes are sufficient to ensure that batch job processing is managed adequately, specifically: 1) batch job processing is formally defined and documented; 2) the job failure process is formally defined, specifically, the root-cause analysis process that includes log, alerts, and job status reports to evaluate job process failure causes. 3) job failure process includes a defined recovery strategy, including required testing, results documentation, and communication to key stakeholders.	
8) <u>Customer Contact Center Call Capacity Monitoring</u>	
Rating: 3	
<u>Risk:</u> Potential that the maximum number of calls capacity is exceeded resulting in dropped calls and customer inability to obtain support during emergency situations.	

<u>Observation:</u> The Genesys application utilizes ports (uniquely identified telephony objects) to handle customer calls; the maximum number of ports for NiSource is currently set to 360, and port capacity (e.g., the number of simultaneous calls handled by these ports or capacity against predetermined threshold) is not monitored.	<u>Management Action Plan:</u> Port capacity and call routing will be addressed and updated by IT Applications management as part of the current IVR Refinements project, resulting in unlimited port capacity. <u>Responsible:</u> Viji Jagabandhu, Director Transformation Delivery <u>Resolution Date:</u> July 2024
<u>Evaluation Criteria:</u> Controls and processes are sufficient to ensure that call capacity monitoring processes are defined and managed to support customer needs; specifically: 1) call capacity processes and limitations are formally defined; 2) call capacity monitoring practices are defined, performed, and reviewed on a periodic basis; 3) call capacity reporting is defined and shared periodically with key stakeholders.	
9) <u>Customer Contact Center Applications Alert Management</u>	
<u>Risk:</u> Potential that IT customer contact center support teams are not timely notified of key application failures and are not able to provide adequate support to customers.	
<u>Observation:</u> Key customer contact center applications (including Genesys, NICE, and VHT) have the ability to alert key IT and business stakeholders of application failures. These alerting systems are configured to send e-mail notification messages to specified recipients when an error within an application occurs. While these alerts are enabled for these applications to send e-mail notifications during application failures, the alerts are configured based on predetermined vendor default settings and have not been evaluated for applicability or customization to NiSource's requirements.	A management response is not requested; however, IA recommends that IT Applications management and Customer Contact Center management align on alert system management capabilities and expectations, and update alerting as applicable based on the results.
<u>Evaluation Criteria:</u> Controls and processes are sufficient to ensure that IT and customer contact center support are timely notified of system errors and failures in order to support customer needs; specifically: 1) customer contact center applications alerts and monitoring are configured according to NiSource's requirements and setup expectations; 2) current alert setup is reviewed to ensure all configurations are enabled for application errors and functionality; 3) current alert e-mail notification is structured to ensure all key stakeholders are notified of application failures based on their support role.	



Internal Audit Department



We exist to deliver safe, reliable energy that drives value to our customers

NiSource Corporate Services Company Key Vendor Governance

Internal Audit Report

Distribution

Respondents:

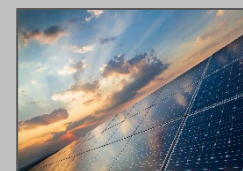
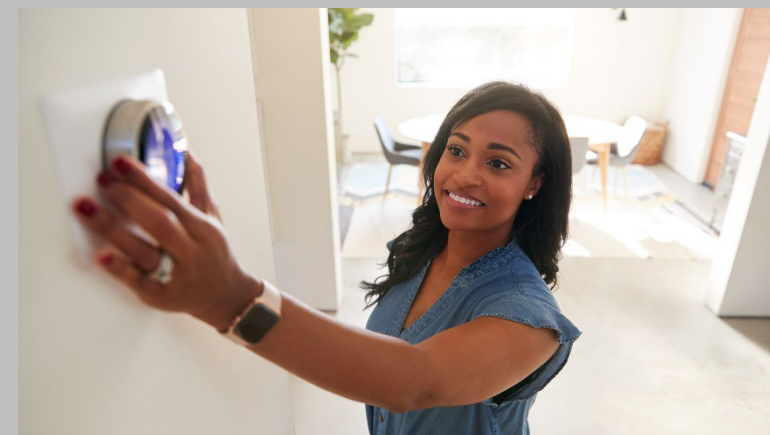
Doug DeBaltzo
Jason Griffith
Tonja Langhurst
Sheena Metzger
Crystal Miller

Beneficiaries:

Waco Bankston
Percell Berry
Sandra Brummitt
Matt O'Donnell
Greg Oliver

For Information:

Shawn Anderson
Melanie Berman
Melody Birmingham
Donald Brown
Kim Cuccia
William Jefferson
Michael Luhrs
Lloyd Yates



Executive Summary

Key Insights

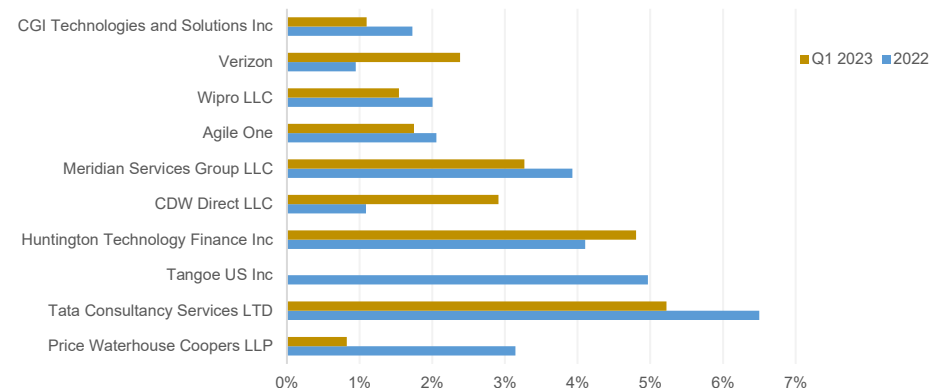
- The Supply Chain team recently rolled out a revised source to pay policy, which clarifies some requirements associated with governance over third-party vendors; however, third-party risk management (TPRM) activities at NiSource Inc. (NiSource or the Company) are currently dispersed across various functions, and the Company's TPRM framework is immature
- A decentralized structure, misalignment regarding responsibilities and expectations, and inadequate tools and processes to share vendor risk and performance information across organizational boundaries impairs some vendor governance and TPRM activities
- Continued promulgation of policy requirements and advancing an enterprise TRPM framework, including improving tools and processes, would facilitate more efficient and effective vendor oversight and TPRM

Key Background Information



Indirect controllable spend totaled \$560 million (18% of total controllable spend) with 2,023 vendors in 2022 and \$171 million (25% of total controllable spend) with 957 vendors through Q1 2023

Top Vendors by % of total Indirect Controllable Spend



Count of Audit Findings by Scope Area

Contract Monitoring/Management	2	Rating 1
Vendor Oversight	No Findings	Rating 2
Compliance Monitoring	No Findings	Rating 3
Performance Monitoring	2	
Incident/Issue Resolution Management	No Findings	
Invoiced Cost Validation	1	

Note: Less-significant observations were discussed with management during the audit.

Audit Approach & Coverage

We conducted a risk-based evaluation of the adequacy, effectiveness, and efficiency of controls associated with vendor governance and performance management activities related to the Company's top ten indirect vendors by spend. Activity evaluated for this audit occurred during the period between August 2021 and May 2023.

We did not evaluate controls assessed during the Source to Pay audit completed earlier in 2023.

Summary of Findings

1) **Contractually Defined Performance Metrics** (Rating 2)

Appropriate vendor performance metrics are not always negotiated and included within executed contracts and processes to ensure that performance clauses included in contracts are periodically validated and amended when necessary are informal and inconsistent.

2) **Vendor Contract Duration Monitoring** (Rating 2)

Prior to the implementation of NiSource's revised source to pay policy, contract duration limits were not established, and a process was not initiated to identify and address inappropriate contract duration terms for contracts executed prior to the policy revision.

3) **Vendor Governance and Performance Management Roles & Responsibilities** (Rating 2)

Roles, responsibilities, and expectations regarding vendor performance management activities are not consistently understood, resulting in inadequate or inconsistent execution.

4) **Purchasing Document Requirements** (Rating 2)

The Company's source to pay policy guidance is insufficient related to which purchasing documents should be used to ensure the contractual protections established are appropriate in consideration of the particular scope of the agreement.

5) **Contractually Defined Financial Penalties Collection Processes** (Rating 2)

Company policy does not specify requirements for waiving contractually defined financial penalties and modifying defined financial penalties related to vendor performance metrics within established contracts.

"1" Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company's reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

"2" Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

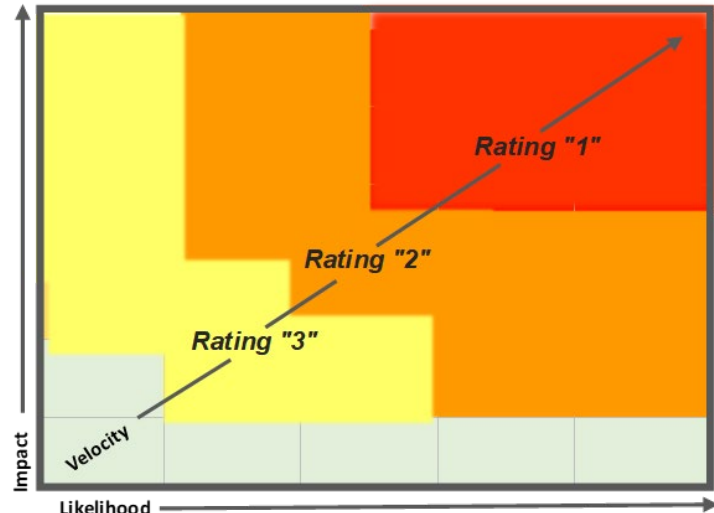
- More than remote probability for damage to the Company's reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

"3" Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

"4" Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited



1) <u>Contractually Defined Performance Metrics</u>	Rating: 2
<u>Risk:</u> Potential that inadequate or irrelevant performance metrics within executed contracts impairs NiSource Inc.'s (NiSource or the Company) ability to drive and monitor vendors' performance and recover or offset increased costs associated with poor vendor performance.	
<u>Observation:</u> Appropriate vendor performance metrics are not always negotiated and included within executed contracts. Additionally, processes to ensure that performance clauses included in contracts are periodically validated and amended when necessary are informal and inconsistent. We specifically noted: - Contracts for three (of 10) vendors do not include defined performance metrics to drive the vendors' performance in line with the Company's requirements; total spend related to these three vendors totaled \$53 million in 2022 and \$19 million through Q1 2023 - Contracts for two (of 10) vendors include defined performance metrics; however, due to the evolution of the relationship with the vendor, the metrics are no longer relevant for the current services provided; total spend related to these two vendors totaled \$36 million in 2022 and \$10 million through Q1 2023	<u>Management Action Plan:</u> Supply Chain management noted that the revised source to pay policy (effective January 2023) explicitly requires Supply Chain involvement during the contract negotiation and execution for vendor contracts with anticipated spend in excess of a defined threshold, which would provide additional oversight to ensure relevant and clearly defined performance metrics are included within each vendor contract prior to execution (for both new and renewed agreements). To address contracts executed prior to the implementation of the revised policy, Supply Chain management, in conjunction with business process owners, will develop and execute a plan to review contracts for the vendors identified within this audit to ensure appropriate performance metrics are added during contract renewals (consideration will be given to risk existing for contracts with future renewal dates and additional negotiations will be held as necessary). <u>Responsible:</u> Doug DeBaltzo, Director of Indirect Category Management <u>Resolution Date:</u> A plan to address contracts executed prior to the implementation of the revised policy will be developed by October 2023; dates associated with specific action steps to be identified in the plan are to be determined.
<u>Evaluation Criteria:</u> Processes and controls are in place to ensure that vendor contracts contain appropriate vendor performance expectations and metrics; specifically: 1) draft contracts are reviewed prior to execution by an appropriate NiSource representative to ensure all relevant and necessary performance metrics are included; 2) established performance metrics are periodically reviewed to confirm relevancy; and 3) change management processes are established to ensure contract amendments timely capture necessary updates to performance metrics.	
2) <u>Vendor Contract Duration Monitoring</u>	Rating: 2
<u>Risk:</u> Potential that inappropriate contract durations results in increased third-party risk and financial loss due to the Company's inability to renegotiate terms and address evolving risks (e.g., cybersecurity provisions).	
<u>Observation:</u> Prior to the implementation of NiSource's revised source to pay policy, contract duration limits were not established. While the revised policy (effective January 2023) establishes five years as the maximum duration of a vendor contract and restricts the use of auto-renewal terms, a	<u>Management Action Plan:</u> As part of the management action plans associated with Internal Audit's 2023 review of Source to Pay activities, Supply Chain management is in the process of formalizing a process to monitor the use of perpetual and evergreen contracts.

process was not initiated to identify and address inappropriate contract duration terms for contracts executed prior to the policy revision. The duration limits for two (of 10) contracts exceed five years, and two (of 10) contracts were established with evergreen terms. Spend related to these four vendors totaled \$84 million in 2022 and \$22 million through Q1 2023.	<u>Responsible:</u> Crystal Miller, Director of Supply Chain Strategy and Analytics <u>Resolution Date:</u> These actions have been reported complete and as of the date of this audit are pending Internal Audit validation.
<u>Evaluation Criteria:</u> Processes and controls are in place to ensure that contract durations are in line with Company policy; specifically: 1) contracts are reviewed prior to execution by a NiSource representative to ensure that contract durations are in line with Company policy 2) monitoring has been established to ensure that exceptions of Company policy are identified and appropriately resolved; and 3) contracts established prior to the implementation of policy with identified exceptions are renegotiated to durations that comply with Company policy.	
3) <u>Vendor Governance and Performance Management Roles & Responsibilities</u>	
<u>Risk:</u> Potential that third-party risk is not identified and appropriately managed leading to poor vendor performance that is not timely identified and resolved, resulting in a negative operational, financial, and/or reputational impact.	
<u>Observation:</u> Roles, responsibilities, and expectations regarding vendor performance management activities are not consistently understood, resulting in inadequate or inconsistent execution. We evaluated performance monitoring activities for 10 vendors (associated with total spend of \$176 million in 2022 and \$48 million through Q1 2023) and noted that some business process owner review activities are insufficient. In particular, vendor-provided information to substantiate that performance complies with established metrics was not consistently obtained and validated, or the business owner's review was not adequate or was insufficiently evidenced. Also, escalation processes were not defined to resolve situations where a vendor provides inadequate information.	<u>Management Action Plan:</u> Supply Chain management will perform the following: - Develop and execute a plan to refine documented training and reference materials to clearly define roles and responsibilities over vendor governance and performance management activities (plan to be developed by October 2023; execution of plan to be determined) - Develop and execute a plan to establish training and communication processes (including method of delivery, required frequency, and business owner identification) associated with vendor governance and performance management activities (plan to be developed by October 2023; execution of plan to be determined) - Develop and execute a plan to conduct training and communication processes associated with vendor governance and performance management activities (plan to be developed by October 2023; execution of plan to be determined) The Information Technology (IT) Service Management team will perform the following by December 2023: - Refine existing processes to ensure the IT Governance team receives confirmation of completed validation activities from the NiSource IT Tower leads within a set timeframe

	Conduct training over refined process requirements with all NiSource IT Tower leads IT Infrastructure will execute performance management activities for the identified vendor contracts (Tangoe) to validate performance aligns with contractually defined metrics (August 2023). HR Operations will execute performance management activities for the identified vendor contract (Agile One) to validate performance aligns with contractually defined metrics (July 2023). Indirect Category Management Supply Chain will develop and execute a plan to address performance management activities for the identified vendor contract (Tata Consultancy Services Evolution of Business Services) to validate performance aligns with contractually defined metrics (plan to be developed by October 2023; execution of plan to be determined). <u>Responsible:</u> Doug DeBaltzo, Director of Indirect Category Management Jason Griffith, Director of IT Infrastructure Tonja Langhurst, Director of HR Operations Delivery Sheena Metzger, Director of IT Business Management <u>Resolution Date:</u> Refer to target remediation dates above.
<u>Evaluation Criteria:</u> Processes and controls are sufficient to ensure that vendor performance issues are identified and appropriately addressed; specifically: 1) roles and responsibilities for monitoring and metric validation are clearly defined and understood; 2) performance metrics are timely reviewed and instances of non-compliance are appropriately addressed and financial penalties are assessed and collected; 3) escalation processes associated with issue resolution are defined and understood; and 4) oversight activities are sufficient to ensure business process owners are effectively executing vendor performance management responsibilities.	
4) <u>Purchasing Document Requirements</u>	Rating: 2
<u>Risk:</u> Potential that company spend is not appropriately pre-approved, resulting in financial loss or reputational risk.	
<u>Observation:</u> The Company's source to pay policy requires the execution of appropriate purchasing documents for spend in excess of a specified threshold (\$100,000 under the updated policy as of January 2023 and \$250,000 prior to January 2023). However, the policy guidance is insufficient related to which purchasing documents should be used to ensure the contractual protections established are appropriate in consideration of the particular scope of the agreement. We specifically identified four vendors were paid a total of \$65 million for consulting services and technology	<u>Management Action Plan:</u> As part of the management action plans associated with Internal Audit's 2023 review of Source to Pay activities, Supply Chain management is in the process of performing the following: Establish monitoring around purchasing documents associated with vendor spend (Reported Complete as of June 2023)

equipment, and the appropriate purchasing documents were not executed.	• Modify the existing source to pay policy to clarify expectations around the use of purchasing documents (August 2023) • Conduct a read and acknowledge training on the revised source to pay policy for the entire Company (August 2023) <u>Responsible:</u> Doug DeBaltzo, Director of Indirect Category Management Crystal Miller, Director of Supply Chain Strategy and Analytics <u>Resolution Date:</u> Refer to target remediation dates above.

Evaluation Criteria:

Processes and controls are sufficient to ensure the Company is adequately protected and spend is appropriately controlled and assessed based upon the nature of the transaction; specifically: 1) purchasing expectations and requirements, including when to create appropriate purchasing documents, have been formalized within a company policy that is communicated to employees; 2) employees are appropriately trained on revised policy expectations; 3) employees have the ability to access the appropriate purchasing documents to support the spend and further ensure that the spend is in alignment with our contractual obligations; and 4) monitoring activities are in place to identify instances of potential non-compliance with policy or contractual terms.

5) Contractually Defined Financial Penalties Collection Processes

Rating: 2

Risk:

Potential that financial penalties are not collected in a timely manner or are waived by an employee without proper authorization, resulting in financial loss.

Observation:

Company policy does not specify requirements for waiving contractual penalties or modifying defined financial penalties related to vendor performance metrics within established contracts, increasing the risk that business decisions may be made without proper levels of oversight and review.

We specifically noted penalties totaling approximately \$185,000 resulting from insufficient performance against contract terms for one IT Services vendor for the months of September and October of 2022 were outstanding as of January 2023.

Management Action Plan:

Supply Chain management will perform the following:

- Identify which Company policy should define requirements associated with contractual penalty activities, including penalty waivers and collection processes (October 2023)
- Formalize requirements associated with contractual penalties within established Company policy (TBD – dependent upon execution of first item)
- Conduct training on the revised policy requirements for impacted employees (TBD – dependent upon execution of second item)

Responsible:

Doug DeBaltzo, Director of Indirect Category Management

Resolution Date:

Refer to target remediation dates above.

Evaluation Criteria:

Processes and controls are sufficient to ensure financial penalties are appropriately calculated and collected and are subject to the appropriate level of oversight; specifically: 1) there is monitoring in place over the critical performance indicators (CPI's) to identify instances of non-compliance by our vendors; 2) there is an appeal process in place to allow the vendor the opportunity to present a case to the Company for performance issues that are not within the vendor's control; 3) an internal review of the appeals occur and documented decisioning is in place; 4) there is a policy in place that defines the appropriate escalation and review process when waiver of financial penalties is being considered; 5) there is monitoring in place to identify instances of non-compliance with the documented waiver escalation and approval process and 6) when financial penalties are due from a vendor there is system functionality in place to ensure that invoice payment does not occur until receipt of financial credits due from the vendor.

6) Preferred Supplier Designation

Rating: 4

Risk:

Potential that having multiple preferred suppliers that provide similar services increases the cost of contract negotiation and reduces the Company's bargaining power across suppliers.

Observation:

The Company utilizes preferred suppliers to drive consistency, efficiency, and cost savings across business units by negotiating favorable terms for pricing and delivery. These suppliers are identified and managed by Supply Chain; however, Supply Chain has not established minimum spend percentage allocation targets when there are multiple preferred suppliers within higher risk categories potentially impacting projected costs savings and efficiencies.

A management response is not requested; however, Internal Audit recommends that management:

- Perform a one-time review of the Company's established preferred suppliers to identify high risk categories with more than one preferred supplier
- Establish, communicate and monitor minimum spend percentage allocation targets for the high risk preferred supplier categories that have multiple preferred suppliers

Evaluation Criteria:

Processes and controls are in place relating to the identification and use of preferred suppliers to ensure that the expected synergies and cost savings are achieved; specifically: 1) a documented review is performed to ensure that the preferred supplier designation is appropriately assigned; 2) a periodic evaluation of preferred suppliers is performed to ensure that it is still relevant to the Company; 3) designation of strategic suppliers occurs for categories that have more than one preferred supplier; and 4) minimum thresholds are established for preferred suppliers that are not identified as strategic suppliers.



Internal Audit Department



We exist to deliver safe, reliable energy that drives value to our customers

NiSource Corporate Services Company Remote Access & Firewall Security Controls

Internal Audit Report

Distribution

Respondents:

Jason Griffith
Jeremy Plante

Beneficiaries:

Carla Donev
Percell Berry

For Information:

Shawn Anderson
Melanie Berman
Melody Birmingham
Donald Brown
Kim Cuccia
William Jefferson
Michael Luhrs
Lloyd Yates



Executive Summary

Key Insights	Key Background Information
- While NiSource Inc. (NiSource or the Company) has an established network security team, certain network security roles and responsibilities have been historically outsourced to a third-party provider (including three consecutive service providers, the most recent being Wipro) and the continuous handoffs in third-party providers performing these activities has negatively impacted adherence to best practices and has introduced challenges with implementing more restrictive network access control policies - Cybersecurity Network management plans to implement the virtual private network (VPN) to be always on effective December 2023, which will improve the corporate network security environment by ensuring users cannot circumvent established controls and introduce vulnerabilities to the Company's technology environment	 53 firewalls deployed in the NiSource environment, with two redundant firewalls deployed for egress traffic in the Hammond, IN and Columbus, OH (Arena) locations  Nearly 8,700 users with remote access to the corporate network through VPN (88%) or virtual desktop (12%)  Approximately 1,300 web applications accessible to corporate end-users

Count of Audit Findings by Scope Area

Remote Access Controls		Firewall Security	
*The finding overlaps in scope areas			
Remote Access Control and Authorization Management	1	Port Restrictions and Rulesets Configuration	1
Encryption Management	No Findings	Application-level Firewall Security	1
Access Control Point Management	1*	Logging Activities	No Findings
Privileged Commands Management	No Findings	Firewall Vulnerability, Patch, and Update Processes	1* 1
Protection of Mechanism Information	No Findings	DMZ and Routing Configuration	1
Disable Access Capability Configuration	No Findings	Firewall Continuity/Availability Management	No Findings
Unauthorized Connection Monitoring	No Findings		

Note: Less-significant observations were discussed with management during the audit.

Audit Approach & Coverage

We co-sourced with PricewaterhouseCoopers LLP (PwC) to conduct a risk-based evaluation of the adequacy and effectiveness of procedural and systemic controls associated with NiSource's corporate remote access and firewall security environments.

PwC did not evaluate controls related to the Operational Technology (OT) or Industrial Controls Systems (ICS) environments during this audit.

Summary of Findings

1) Firewall Access Control Lists (Rating 1)

Processes and controls are not in place to periodically review Access Control List (ACL) rules to ensure they are configured to appropriately restrict network traffic; as a result, internet-facing and internal firewalls have been configured with overly permissive firewall rules that allow network traffic over 'any' Application and 'any' Service, which may expose the network to unauthorized access.

2) Network Device Patch and Vulnerability Management Controls (Rating 1)

Processes to identify vulnerabilities and the related risks associated with delaying patches for firewalls and NiSource's VPN (Cisco ASA) are inadequate; as a result, one Cisco ASA VPN appliance and ten Palo Alto firewalls were running outdated software versions susceptible to several high severity vulnerabilities.

3) Web Application Firewall Coverage (Rating 2)

Web traffic learnings from web application firewall (WAF) objects have not been reviewed to determine and operationalize necessary WAF object rule configurations resulting from the web traffic observations.

4) Off-VPN Remote Access Controls (Rating 2)

The VPN is not configured to be always on and as a result, users are not protected through URL content filtering when they are not connected to the VPN; additionally, users are unable to receive software patching when not connected to the VPN.

5) Network Device Hardening and Configuration Best Practices (Rating 2)

Information Technology (IT) standards for network device hardening configuration within the corporate network environment have not been developed and aligned with industry minimum baseline security standards to prevent an attacker from taking advantage of a misconfigured or compromised firewall.

6) Network Architecture Design (Rating 3)

Non-proxied web traffic, including VPN traffic for mobile devices, is allowed through the DMZ interface, which is contrary to the recommended best practice of segregating interfaces by tiers to protect the internal network from security vulnerabilities and detect anomalous network traffic.

"1" Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company's reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

"2" Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

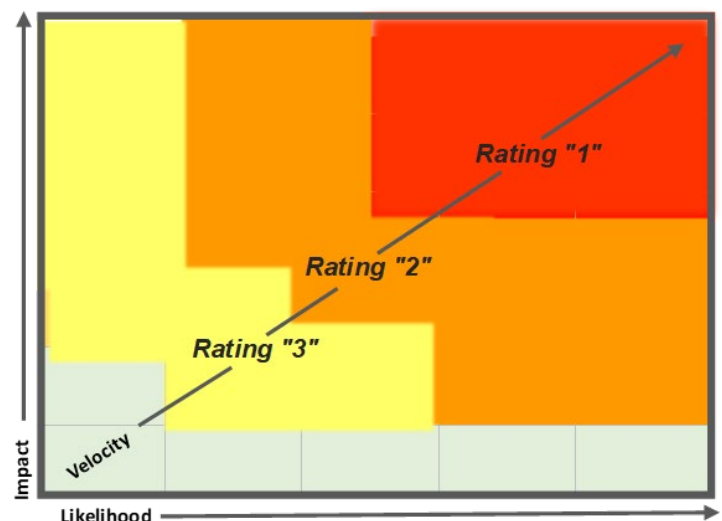
- More than remote probability for damage to the Company's reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

"3" Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

"4" – Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited



1) <u>Firewall Access Control Lists</u>	Rating: 1
Risk: Potential for unauthorized access or exfiltration of confidential/sensitive data/information.	
Observation: NiSource Inc. (NiSource or the Company) uses Palo Alto firewalls configured with Access Control List (ACL) rules to prevent unauthorized users from accessing Company resources and restrict authorized users' access to specific resources. ACL rules are not periodically reviewed to ensure they are configured to appropriately restrict network traffic. The audit team specifically identified the following: • Ten (of 10) firewalls have a combined 55 firewall rules that allow traffic over "any" application and "any" service, which has resulted in more restrictive ACL rules being negated • Ten (of 10) firewalls have a combined 62 firewall rules that allow traffic of named applications over "any" service instead of the "application-default" configuration • Two internet-facing Edge firewalls have rules configured to allow network traffic from the demilitarized zone (DMZ) to the Inside zone for an 'unknown-udp' application and 'any' service	Management Action Plan: Cybersecurity Network management will perform the following: • Develop a process to systematically review all firewall rules across the identified devices; the plan will detail the methodology, frequency, and scope of the review (December 2023) • Execute a process to annually review the firewall rules to validate the necessity and appropriateness of each rule to ensure that outdated or overly permissive rules are identified and modified or removed as needed (February 2024) Responsible: Jeremy Plante, Director Cybersecurity Resolution Date: Refer to the target remediation dates for each action item listed above.
Evaluation Criteria: Processes and controls are sufficient to ensure all firewalls are configured to restrict inbound and outbound network traffic; specifically: 1) changes to firewall access control rules are restricted to authorized network security personnel and third parties; 2) changes to firewall access control rules are subject to change control review and approval processes; 3) firewall rulesets are periodically reviewed to remove rules that are no longer necessary or negate more restrictive rules; 4) network access control lists are in place to enable authorized traffic between internal subnets; and 5) access to and from the public internet is restricted.	
2) <u>Network Device Patch and Vulnerability Management Controls</u>	Rating: 1
Risk: Potential that external-facing and internal firewalls are open to vulnerabilities that are susceptible to exploitation and bypass existing network security controls.	
Observation: The NiSource Cybersecurity Network team utilizes a third-party (Wipro) to manage certain processes for firewalls and NiSource's virtual private network (VPN) (Cisco ASA), including patching and updating configurations rules. To reduce the probability of outages related to the introduction of newly developed and possibly not fully stress-tested technology, the NiSource Cybersecurity Network team has instructed Wipro to apply firewall and Cisco ASA software patches utilizing an n-1 model (which means keeping the NiSource environment one version behind the most currently available version). However, processes to identify vulnerabilities and the related risks associated with delaying patches for firewalls and Cisco ASA are	Management Action Plan: Cybersecurity Network management will perform the following: • Execute prioritized patching of the identified high severity vulnerabilities on Cisco ASA, the internet-facing Edge firewalls, and internal firewalls; the focus will be on mitigating the most critical vulnerabilities • Implement a periodic (monthly or as deemed appropriate based on risk profile) and comprehensive vulnerability scanning schedule for all firewall devices to identify vulnerabilities early and aid in prioritization for patching

inadequate. As a result, the audit team specifically identified the following: - NiSource is running an outdated version of Cisco ASA (n-3 at the time of the audit) that may be susceptible to 16 high severity vulnerabilities - Two internet-facing Edge firewalls (n-10 at the time of the audit) may be susceptible to seven high severity vulnerabilities - Eight internal firewalls (n-16 at the time of the audit) may be susceptible to 20 high severity vulnerabilities	- Establish periodic touch points with the third-party provider (Wipro) to ensure they are aligned with NiSource's security priorities and patching strategies and implement necessary training, awareness sessions, or joint reviews of the patching process as deemed appropriate IT Infrastructure management will perform the following: - Decommission the Cisco ASA VPN once the Palo Alto VPN has been implemented Responsible: Jason Griffith, Director IT Infrastructure Jeremy Plante, Director Cybersecurity Resolution Date: January 2024
Evaluation Criteria: Processes and controls are sufficient to ensure that all network and infrastructure devices within the NiSource environment are covered by patch and vulnerability management processes; specifically: 1) network and infrastructure devices are regularly scanned for vulnerabilities; 2) processes are in place to regularly deploy patches to network and infrastructure devices; 3) vulnerabilities that are not patched are documented, approved, and periodically reviewed; and 4) an asset inventory exists that inventories the firewalls in use, including the version of firmware.	
3) <u>Web Application Firewall Coverage</u>	
Risk: Potential for an attacker to gain unauthorized access to NiSource data by exploiting vulnerabilities of public-facing applications and services.	
Observation: NiSource maintains approximately 40 public-facing virtual IP addresses (VIPs) that sit behind Hypertext Transfer Protocol (HTTP)/Hypertext Transfer Protocol Secure (HTTPS) load balancers to distribute the processing and communications activity evenly across servers within the Company's network. These load balancers are configured to enable web application firewall (WAF) objects to provide security controls at the application layer and timely identification of malicious network traffic. The WAF objects have been set to monitor network traffic going to these VIPs in learning mode since their implementation in October 2022; however, the web traffic learnings are not periodically reviewed to determine and operationalize necessary WAF object rule configurations resulting from the web traffic observations.	Management Action Plan: Cybersecurity Network management will perform the following: - Conduct a review of the learning mode data collected from the WAFs to identify patterns, anomalies, or potential threats based upon the observations - Perform staff training for depth of talent - Using the insights from the review of the learning mode data, configure WAF rules to actively block or challenge suspicious or malicious traffic to ensure WAFs are actively defending the applications - Establish a periodic process (quarterly or as deemed appropriate based on the risk profile) to review the WAF rules and optimize the rules based on changing threat landscapes and application behaviors Responsible: Jeremy Plante, Director Cybersecurity

		<u>Resolution Date:</u> March 2024
<u>Evaluation Criteria:</u> Processes and controls are sufficient to ensure WAFs offer adequate protection to public-facing web applications or services; specifically: 1) WAFs are on the network boundary; 2) WAFs are configured to monitor web traffic for security threats at the application layer; 3) WAFs are configured to block known malicious or suspicious traffic; and 4) WAFs are periodically monitored to ensure WAF settings are optimized.		
4) <u>Off-VPN Remote Access Controls</u>		Rating: 2
<u>Risk:</u> Potential that end-users download malware on NiSource assets or visit a malicious website or personal file sharing sites (e.g., Box, Gmail) that are not blocked through URL filtering controls, which could have a negative impact to the Company's systems or data.		
<u>Observation:</u> NiSource assets used by end-users (e.g., workstations) are configured with CrowdStrike Endpoint Detection and Response (EDR) agents and uniform resource locator (URL) content filtering controls to monitor for and prevent for web-based threats. While URL filtering controls are in place when the asset is connected to the VPN, the VPN is not configured to be always on. As a result, users are not protected through URL content filtering when they are not connected to the VPN. Additionally, users are unable to receive software patching through the Microsoft System Center Configuration Manager (SCCM) when not connected to the VPN.	<u>Management Action Plan:</u> NiSource is already in the process of implementing GlobalProtect's always-on VPN solution. Cybersecurity Network management will prioritize its rollout to all users to ensure that assets are always connected to the VPN when accessing the internet, benefitting from the URL content filtering and other security controls. As part of this project, IT Infrastructure management will decommission the Cisco ASA VPN.	
		<u>Responsible:</u> Jeremy Plante, Director Cybersecurity Jason Griffith, Director IT Infrastructure
		<u>Resolution Date:</u> December 2023
<u>Evaluation Criteria:</u> Processes and controls are sufficient to ensure preventive security controls are in place to protect endpoints when a user is not connected to the VPN; specifically: 1) EDR and/or Anti-Malware agents are deployed to endpoints; 2) the NiSource Cybersecurity Network team is able to deploy actions to devices that are connected to the internet and are off the VPN network, such as pushing security updates; and 3) URL content filtering controls are in place.		
5) <u>Network Device Hardening and Configuration Best Practices</u>		Rating: 2
<u>Risk:</u> Potential that the misconfiguration of firewall devices may leave the internal network environment susceptible to known network security threats.		
<u>Observation:</u> Company Information Technology (IT) standards for network device hardening configuration within the corporate network environment have not been developed and aligned with industry minimum baseline security standards (e.g., Center for Internet Security (CIS) Benchmarks). As a result, processes and controls are insufficient to prevent an attacker from taking advantage or a misconfigured or compromised firewall; specifically:	<u>Management Action Plan:</u> Cybersecurity Network management will perform the following: Establish comprehensive network device hardening standards based upon recognized industry standards (e.g., CIS benchmarks) which encompass all facets of device configuration, from session timeouts to password policies	

- While periodic security operations optimization assessments are conducted, processes and procedures have not been established to dictate the frequency of firewall configuration setting reviews and how to address findings identified through these assessments - Ten (of 10) firewalls have default idle session timeouts of 60 minutes, which deviates from industry standards of ten minutes - Ten (of 10) firewalls are not configured to enforce a password age policy and eight (of 10) firewall devices are not configured to enforce password complexity policies aligned to industry standards - Four (of 10) firewalls did not have time synchronization configured, which is not aligned to industry standards	- Modify the session timeouts on the ten identified firewalls to adhere to the industry standard of ten minutes - Implement password age and complexity policies on the ten identified firewalls to adhere to industry best practices - Ensure all firewalls have time synchronization configured to maintain accurate logging and operational consistency Additionally, Cybersecurity Network management will explore the opportunity to utilize a configuration management tool to help in monitoring and managing firewall configurations in real-time, including alerting on deviations from the baseline <u>Responsible:</u> Jeremy Plante, Director Cybersecurity <u>Resolution Date:</u> The network device hardening standards will be established by March 2024. All other action plans will be completed by April 2024.

Evaluation Criteria:

Processes and controls are sufficient to ensure that the configuration settings of firewall devices are standardized across the NiSource environment and adhere to industry leading practices; specifically: 1) formal firewall hardening standards are in place; and 2) firewalls are periodically audited to detect any deviations from established standards (e.g., configuration drift).

6) Network Architecture Design

Rating: 3

Risk:

Potential for reduced network security and monitoring capabilities due to inadequate segregation of network interfaces on egress firewalls.

Observation:

The egress (outbound) firewalls currently permit non-proxied web traffic, including VPN traffic for mobile devices not associated with the corporate network, to traverse through the DMZ interface. This configuration deviates from established best practices that recommend the segregation of network interfaces by tiers (e.g., have dedicated interfaces for application traffic, web traffic, VPN traffic). As a result, the current configuration allows traffic that may not be appropriately segmented or separated, potentially exposing the internal network to security vulnerabilities and reducing the ability to detect anomalous network traffic.

Management Action Plan:

Cybersecurity Network management will perform the following:

- Conduct a thorough assessment of the current network architecture, especially focusing on the egress firewalls, to identify all traffic flows and segregate them based on their intended purposes (May 2024)
- Reconfigure the egress firewalls to segregate traffic by tiers, ensuring dedicated interfaces for different types of traffic (e.g., application traffic, proxied traffic, VPN traffic)
- Implement monitoring tools to observe each traffic flow to help in quickly identifying and responding to anomalies or potential security threats

	<u>Responsible:</u> Jeremy Plante, Director Cybersecurity <u>Resolution Date:</u> May 2024
<u>Evaluation Criteria:</u> Processes and controls are sufficient to ensure that egress firewalls are configured to properly segment network traffic based on their intended purposes; specifically: egress firewalls are configured with interfaces dedicated for application traffic, proxied web traffic, VPN traffic, etc.	



Internal Audit Department



We exist to deliver safe, reliable energy that drives value to our customers

NiSource Inc. Payroll General Controls

Internal Audit Report

Distribution

Respondents:

Kristen King
Leslie Lancione
Tonja Langhurst
Greg Oliver
Anna Ortega

Beneficiaries:

Daniel Dring
Gunnar Gode

For Information:

Shawn Anderson
Melanie Berman
Melody Birmingham
Donald Brown
Kim Cuccia
William Jefferson
Michael Luhrs
Lloyd Yates



Executive Summary

Key Insights

- The Human Resources and Payroll Operations teams perform various activities to ensure payroll is timely and accurately paid; however, the success of some critical activities is reliant upon the knowledge and expertise of the employees performing the task, and established reviews are sometimes performed by employees without the knowledge and experience that enables identification of issues within the process
- While controls are established over the accuracy and completeness of payroll transactions, some controls are not executed at the appropriate point in the process to appropriately mitigate risk

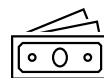
Key Background Information



\$2.0 billion in payroll expense for January 2023 – August 2023



7,349 employees (2,517 union employees and 4,832 non-union employees)



Five pay groups, with payroll being executed at varying intervals (e.g., bi-weekly and monthly pay cycles)

Count of Audit Findings by Scope Area

Payroll Policies and Procedures	No Findings	Rating 1
Payroll Processing Controls	2	Rating 2
Vender Oversight	1	Rating 3
Payroll Deductions and Employee Contribution	No Findings	
Comp. Factors (including Union Employees)	1	
Regulatory Reporting and Compliance	No Findings	
Accounting Controls	1	

Audit Approach & Coverage

We conducted a risk-based evaluation of the adequacy, effectiveness, and efficiency of controls associated with payroll activities. Transactions evaluated for this audit occurred during the period between January 2022 and August 2023.

We did not evaluate performance management controls associated with activities performed by Tata Consultancy Services (TCS) as these activities were reviewed as part of the key vendor governance audit performed earlier in 2023.

Note: Less-significant observations were discussed with management during the audit.

Summary of Findings

1) **Union Employee Compensation Controls (Rating 2)**

Some key activities that impact union employees' pay are decentralized, and monitoring controls are inadequate to ensure these employees are always appropriately paid.

2) **Off-Cycle Payroll Payment Controls (Rating 2)**

While in practice the duties of initiating, funding, and distributing payment cards (used to make off-cycle, one-time payments to employees) are segregated, procedures to manage and review access to the associated bank portal are inadequate, which could result in inappropriate access to the portal, which can be accessed outside of the Company's network; additionally, monitoring controls are inadequate to timely identify activity that is potentially inappropriate; we did not identify any inappropriate activities.

3) **Human Resources and Payroll Operations Risk and Control Framework (Rating 2)**

The current Sarbanes-Oxley (SOX) control framework and scope of testing performed should be enhanced.

4) **Payroll Accounting Controls (Rating 2)**

While management performs various analytical procedures to ensure that accrued payroll is materially correct, NIPSCO accrued payroll account reconciliation procedures are insufficient; specifically, identified large reconciliation variances were not adequately reviewed, analyzed, and resolved.

5) **Payroll Vendor Risk Management Activities (Rating 3)**

Third-party vendor controls related to applications where sensitive employee data may be processed and retained are not formally validated.

"1" Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company's reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

"2" Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

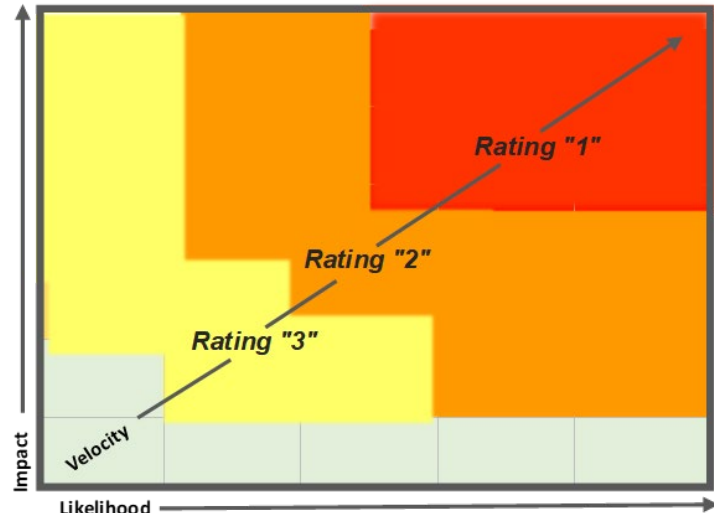
- More than remote probability for damage to the Company's reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

"3" Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

"4" Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited



1) <u>Union Employee Compensation Controls</u>		Rating: 2
<u>Risk:</u> Potential that labor agreement violations can lead to legal action, financial loss and a negative reputational impact for NiSource Inc. (NiSource or the Company).		
<u>Observation:</u> Sixteen labor union contracts are in place codifying certain terms and conditions of employment for the labor union workforce (2,517 employees) across NiSource Inc.'s (NiSource or the Company) six operating companies. Some key activities that impact employees' pay are decentralized, and monitoring controls are inadequate to ensure union employees are always appropriately paid; specifically: - Northern Indiana Public Service Company (NIPSCO) union employees are subject to a positive pay model that requires supervisor approval of employee timecards to receive payment; management disclosed to the internal audit team that due to a technical issue in the time entry system (Workbrain) and the timing of when timecard approvals are reviewed, ~ 50 union employees' timecards were not timely approved in April 2023, which affected these employees' pay - Employees' supervisors are responsible for submitting step progression compensation adjustments; however, monitoring activities are insufficient to ensure adjustments are executed in compliance with the established labor agreements, and we identified some exceptions during our limited, sample-based testing - Processes to review and verify the accuracy of universal compensation adjustments resulting from new or updated labor agreements are manual and insufficient to ensure that the pay rates are always applied correctly within the Human Capital Management system (Workday)		<u>Management Action Plan:</u> Human Resources (HR) and Payroll Operations management is in the process of implementing system adjustments to address the timely approval of union employees' timecards to ensure they are timely paid. Labor Relations and HR Services and Solutions management will partner together to develop and execute a plan to establish enterprise-wide monitoring around union compensation adjustments, including step progressions for union employees to ensure they are timely initiated and processed. Labor Relations management will implement analytical procedures around universal compensation adjustments to ensure all adjustments have been appropriately made per the new or updated labor agreements. <u>Responsible:</u> Tonja Langhurst, Director of HR Operations Delivery Anna Ortega, Director of Labor Relations Greg Oliver, VP HR Services and Solutions <u>Resolution Date:</u> April 2024
<u>Evaluation Criteria:</u> Processes and controls are in place to ensure NiSource is in compliance with all new and established labor agreements; specifically: 1) newly executed labor agreements are subject to review and approval by an appropriate Company representative; 2) review/approval controls are established to ensure compensation is in line with the appropriate labor agreement; 3) formalized change management processes are in place over the application of new rates; 4) monitoring is in place to ensure continued compliance with the labor agreements; and 5) instances of non-compliance identified by the Company are timely investigated and appropriately resolved.		
2) <u>Off-Cycle Payroll Payment Controls</u>		Rating: 2
<u>Risk:</u> Potential for misappropriation of assets by Company employees resulting in financial loss.		
<u>Observation:</u> Payment cards are utilized by the Payroll Operations team to make certain off-cycle, one-time payments to employees		<u>Management Action Plan:</u> Payroll Operations management will perform the following:

(total paid January – September 2023 is \$167,000). While in practice the duties of initiating, funding, and distributing payment cards are segregated, procedures to manage and review access to the associated bank portal, which can be accessed outside the Company's network, are inadequate. Additionally, monitoring controls are inadequate to timely identify activity that is potentially inappropriate. At the time of the audit, one former employee had administrator access to the bank portal; this access was subsequently removed. We did not identify any inappropriate activity.	- Enhance review controls around access to the associated bank portal, including controls around timely removal of terminated employees or employees who have transitioned to new roles (e.g., within 24 hours as required per Company policy) - Formally separate or restrict the responsibility of initiating and funding/distributing the Visa cards to different employees within the department or implement a systematic approval and monitoring procedures if establishing segregation of duties is not possible Additionally, Payroll Operations management is currently exploring alternative ways to allow for expedient funds delivery to employees. <u>Responsible:</u> Tonja Langhurst, Director of HR Operations Delivery <u>Resolution Date:</u> April 2024

Evaluation Criteria:

Processes and controls are sufficient to ensure that Visa card usage is controlled and managed to prevent misuse; specifically: 1) roles and responsibilities are established to ensure the individuals that have the ability to initiate a Visa card cannot approve and/or distribute; and 2) in cases where segregation of duties is not possible, monitoring is in place to identify potential inappropriate activity.

3) Human Resources and Payroll Operations Risk and Control Framework

Rating: 2

Risk:

Potential that payroll account misstatements are not timely identified and resolved leading to a financial reporting misstatement; also, potential that payroll is not paid completely, accurately, and timely to employees, resulting in legal action, financial loss and a negative reputational impact for the Company.

Observation:

The Human Resources and Payroll Operations department and the Sarbanes-Oxley (SOX) Compliance team are responsible for identifying risks and controls to ensure payroll is calculated and paid completely, accurately and timely and that payroll is recorded completely and accurately within the financial statements. These controls are subject to quarterly testing by the Human Resources and Payroll Operations teams and are subject to review by the SOX Compliance team. The current SOX control framework and scope of testing should be enhanced; specifically:

- Twelve controls (including controls over unapproved timesheet monitoring and data transfer from Workbrain to Workday) are not being executed as designed; in particular: 1) reviews/approvals are not documented; 2) review precision escalation and resolution activities are inadequate, 3) report completeness and accuracy assessments, and 4) segregation of duties are not

Management Action Plan:

Human Resources and Payroll Operations management is currently partnering with the SOX Compliance team to perform a one-time clean-up of the SOX risk and control framework to ensure that the controls as designed/written are aligned with the appropriate risk, reflective of actual practice, and tested accordingly.

Additionally, SOX Compliance management has completed training with the employees within the Human Resources and Payroll Operations department to communicate roles, responsibilities and expectations of process owners and control testers.

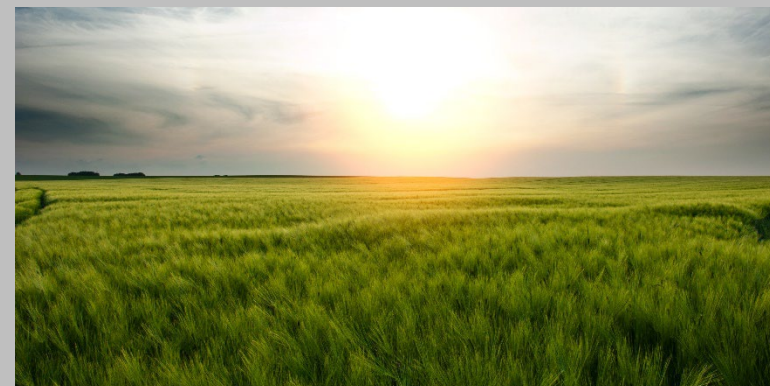
Human Resources and Payroll Operations management will formalize a process to ensure that the controls within the SOX framework are executed as designed to effectively address the risk of incomplete and inaccurate financial statements and at the required points in time.

considered - Three controls (including controls over unapproved timesheet monitoring and role and password monitoring controls for Workday), are only executed when required quarterly SOX testing occurs as opposed to each time the related activity is executed - A formalized and evidenced review is not occurring for seven controls (including controls over the completeness and accuracy of payroll payment reconciliations); as a result, we were unable to validate that a sufficient level of review and oversight was performed - Three controls are not mapped to the appropriate risk the control activity is mitigating within the SOX framework - SOX framework control descriptions for four controls are not reflective of actual practice	SOX Compliance management will formalize the review components within the existing SOX controls and update control testing procedures accordingly. <u>Responsible:</u> Leslie Lancione, Director of HR Optimization and Technology Tonja Langhurst, Director of HR Operations Delivery Kristen King, Director of Consolidations, External Reporting, Technical Accounting & SOX <u>Resolution Date:</u> Human Resources and Payroll Operations will complete their associated action plan items by April 2024. The SOX Compliance team has completed the employee training and will update the SOX framework and testing procedures by April 2024.
<u>Evaluation Criteria:</u> Processes and controls are sufficient to ensure that SOX controls are properly identified, executed and tested to address the risk that payroll is not paid completely, accurately, and timely; specifically: 1) risks and controls are formally identified and codified within the SOX control framework; 2) controls are timely executed and evidenced; 3) controls are tested; and 4) testing is properly documented, including formal sign-off by the process owner and a SOX Compliance team member in the SOX data management application.	
4) <u>Payroll Accounting Controls</u>	
<u>Risk:</u> Potential that payroll account balance misstatements are not timely identified and resolved leading to a financial reporting misstatement.	
<u>Observation:</u> While management performs various analytical procedures to ensure that accrued payroll is materially correct, some of these procedures are not formalized and accrued payroll account reconciliation procedures are insufficient. Specifically, the NIPSCO accrued payroll account balance in the General Ledger is not reconciled to associated subledgers. In addition, large variances identified during the reconciliation process for NIPSCO payroll are not always investigated and resolved. NIPSCO accrued payroll reconciliations for the months of November 2022 and February 2023 contained variances of \$2.0 million and \$1.2 million (21% and 12% of the total account balances), respectively, that were not investigated and resolved prior to quarterly reporting and the variances were not included within the consolidated quarterly variance analysis as is required per policy. Furthermore, controls to validate the data transfer of timekeeping and payroll activities from Workbrain and Workday to PeopleSoft are not performed or included	<u>Management Action Plan:</u> Accounting management will develop and execute a plan to evaluate the control framework for the NIPSCO and CDC accrued payroll account balances and determine necessary actions to address the identified risk, including the potential formalization of existing and in-flight mitigating controls and analytical procedures. <u>Responsible:</u> Kristen King, Director of Consolidations, External Reporting, Technical Accounting & SOX <u>Resolution Date:</u> The plan will be developed by April 2024; dates associated with specific action steps to be identified in the plan are to be determined.

within the SOX framework and testing procedures and as a result, the completeness and accuracy of some of the source information utilized in the CDC accrued payroll reconciliation cannot be verified.	
<u>Evaluation Criteria:</u> Processes and controls are sufficient to ensure the Company's payroll transactions are recorded completely and accurately within the financial statements; specifically: 1) key system functionality within the source systems has been identified and periodically reviewed; 2) data transfer from source system to general ledger is periodically tested to ensure data is transferred completely and accurately; and 3) a periodic reconciliation is performed (including variance review and investigation) and reviewed, comparing an independent source system sub-ledger report to the general ledger.	
5) <u>Payroll Vendor Risk Management Activities</u>	Rating: 3
<u>Risk:</u> Potential that sensitive employee information processed by third parties is inadequately protected resulting in financial exposure and reputational damage.	
<u>Observation:</u> ADP, Inc. (ADP) submitted 249,747 payments for 2022 and 173,555 payments for January – August 2023 on behalf of NiSource to employees. Third-party vendor controls related to applications where sensitive employee data may be processed and retained are not formally validated. Specifically, a service organization control report (SOC 2 Type II) for ADP is not periodically obtained and reviewed to ensure that the vendors' controls are adequate and operating effectively. In addition, normally expected complementary user entity controls (CUECs - which are controls that should be implemented by NiSource), to achieve data protection control objectives are not formalized and validated.	<u>Management Action Plan:</u> Human Resources and Payroll Operations management will formalize and implement a process to periodically obtain and review SOC reports for key vendors, including the implementation and verification of the effectiveness of identified CUECs, as necessary. <u>Responsible:</u> Tonja Langhurst, Director of HR Operations Delivery <u>Resolution Date:</u> February 2024
<u>Evaluation Criteria:</u> Processes and controls are sufficient to ensure risk management activities are being executed for key vendors supporting human resources and payroll operations; specifically: 1) SOC reports and corresponding bridge letters are obtained and reviewed annually by a member of the Payroll team with sufficient knowledge to perform the review; 2) if issues are identified, an evaluation is performed to determine the impact to the Company, including appropriate vendor management risk reduction/resolution activities; and 3) CUECs are reviewed, implemented and verified, as necessary.	



Internal Audit Department



We exist to deliver safe, reliable energy that drives value to our customers

NiSource Inc.

Inventory Management General Controls

Internal Audit Report

Distribution

Respondents:

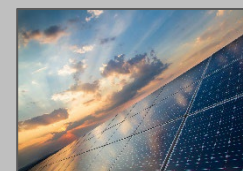
Eric Belle
Kristen King
James Miller
Dave Roy
Kevin Stanley
Jake Upper
Derek Ziolkowski

Beneficiaries:

Waco Bankston
Sandra Brummitt
Carla Donev
Gunnar Gode
William Mojica
Steven Sylvester

For Information:

Shawn Anderson
Melanie Berman
Melody Birmingham
Donald Brown
Kim Cuccia
William Jefferson
Michael Luhrs
Lloyd Yates



Executive Summary

Key Insights	Key Background Information
- NiSource Inc. (NiSource or the Company) outsources inventory management activities for the Columbia Gas Distribution Companies (CDC) to McJunkin Red Man Corporation (MRC); MRC interacts with various departments across the organization, but definition of roles and responsibilities to ensure effective oversight of outsourced activities can be improved - NiSource does not periodically audit MRC activities, nor are independent service organization control (SOC) reports available, which impairs management’s visibility to potential MRC control gaps that could impact NiSource - Northern Indiana Public Service Company (NIPSCO) inventory management activities are performed by internal resources, and the effectiveness of some critical activities is reliant upon the knowledge and expertise of employees performing the tasks as opposed to a reliable control framework	\$157.9 million held in inventory as of August 2023 (\$151.8 million in NIPSCO and \$6.1 million in CDC) \$112.0 million in spend with MRC for 2022 and \$88.3 million for January – August 2023 78 depot locations holding inventory across the five CDC operating states and 28 NIPSCO warehouse locations holding inventory within Indiana
Count of Audit Findings by Scope Area	Audit Approach & Coverage
Vendor Management 2 Inventory Management 1 Payment Validation for Materials Received 1 Inventory Quality Procedures No Findings Physical Security 1 Accounting Controls 1 Rating 1 Rating 2 Rating 3	We conducted a risk-based evaluation of the adequacy, effectiveness, and efficiency of controls associated with inventory management activities. Activity and transactions evaluated for this audit occurred during the period between January 2022 and September 2023. We did not evaluate controls over inventory delivered directly to major project job sites, materials ordering for major projects, or controls related to managing tools and equipment. These activities are being evaluated as part of separate audits occurring during 2023.
Note: Less-significant observations were discussed with management during the audit.	

Summary of Findings

1) Emergency Stock Identification and Management Activities – CDC and NIPSCO (Rating 2)

While an analysis to implement emergency stock processes for steel materials was performed in 2022, inventory risk has not been formally evaluated in consideration of restoration criticality concerns and across all material classes; as a result, the Company has an incomplete understanding of inventory risk, which could lead to delayed restoration of service after a critical event; additionally, controls are insufficient over inventory minimum/maximum levels to ensure adequate inventory levels for components important for ongoing operations.

2) Inventory Accounting Controls – CDC and NIPSCO (Rating 2)

Inventory is not a material component of the Company's total assets, resulting in some associated accounting controls being inadequately performed; specifically, inventory account reconciliation procedures are insufficient and large inventory account reconciliation variances were not adequately investigated and resolved, and reviewed per policy; additionally, controls over key system calculations and data transfers are not performed or included within the Sarbanes-Oxley (SOX) framework and testing procedures.

3) Invoice Accuracy Controls – CDC (Rating 2)

Controls are insufficient to ensure payments to MRC for CDC inventory purchases are per agreed pricing; additionally, materials receiving discrepancies are not timely resolved.

4) Oversight of Inventory Availability – CDC (Rating 3)

NiSource does not ensure that MRC performs contractually required inventory counts at CDC depots; as a result, NiSource does not have visibility to the quantity and locations of all materials physically on hand across the depot locations.

5) Key Performance Indicator Metrics – CDC and NIPSCO (Rating 3)

While key performance metrics for MRC have been established within the vendor contract, NiSource does not perform validation procedures over the vendor-provided performance metric information to ensure that the information is complete and accurate.

6) Physical Security Access Controls – CDC and NIPSCO (Rating 3)

The practice to remove an employee's physical access to company facilities, including depots and warehouses, within 24 hours of termination has not been formalized and documented, and we identified some exceptions through limited, sample-based testing.

"1" Significant Improvement is Needed and Prompt Management Attention is Required

- More than remote probability for damage to the Company's reputation or brand and the impact to the enterprise could be substantial and rapidly realized
- More than remote probability for a non-compliance with laws/regulations and the impact to the enterprise could be substantial and rapidly realized
- Crucial foundational controls related to high-impact processes are inadequate or ineffective and the impact to the enterprise could be substantial and rapidly realized
- Repeat audit findings and the impact could be significant within the scope of the area being audited

"2" Improvement is Needed and Management Attention is Necessary (target to reduce risk within 3 to 6 months)

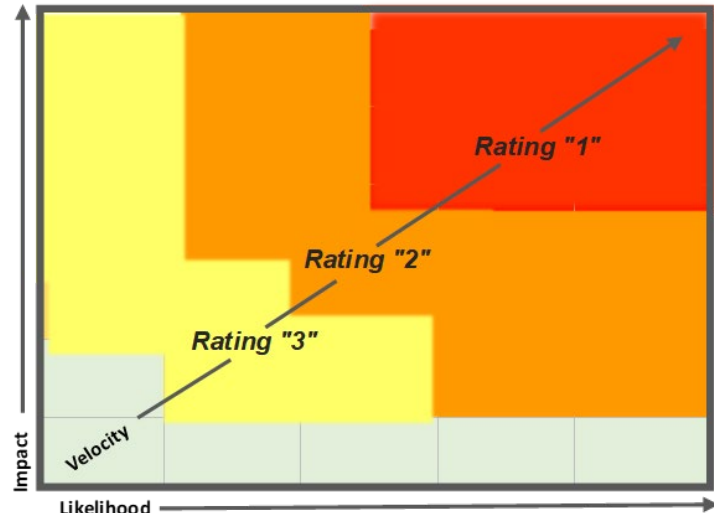
- More than remote probability for damage to the Company's reputation or brand and the impact could be substantial within the scope of the audit
- More than remote probability for a non-compliance with laws/regulations and the impact could be substantial within the scope of the audit
- Foundational controls are inadequate or ineffective and the impact could be substantial within the scope of the audit
- Controls are not adequate to prevent or detect fraud in a timely manner
- Transactional errors identified during audit testing are significant within the scope of the audit (based on value or number of erroneous transactions identified)
- Internal Policy is not adequate or is violated and the impact could be substantial within the scope of the audit

"3" Some Improvement is Needed and Management Attention is Justified (target to reduce risk within 12 months)

- Internal Policy is not adequate or is violated, but impact is limited and the overall system of controls is not significantly compromised
- Controls are not adequate to prevent erroneous transactions and errors could be more than immaterial within the scope of the audit
- Notable lost opportunity or inefficiency within the scope of the audit

"4" Management Evaluation is Desirable

- Isolated exception with limited impact
- Lost opportunity or inefficiency, but impact is limited



1) <u>Emergency Stock Identification and Management Activities (Columbia Gas Distribution Companies (CDC) and Northern Indiana Public Service Company (NIPSCO))</u>	Rating: 2
<u>Risk:</u> Potential that NiSource Inc. (NiSource or the Company) does not have the necessary materials on hand to manage operations or timely restore service following an emergency resulting in extended customer outages that damage the Company's reputation.	
<u>Observation:</u> While an analysis to implement emergency stock processes for steel materials was performed in 2022, inventory risk has not been formally evaluated in consideration of restoration criticality concerns and across all material classes; as a result, the Company has an incomplete understanding of inventory risk, which could lead to delayed restoration of service after a critical event. In addition, inventory components important for ongoing operations are not formally identified and periodically verified by NiSource personnel. While minimum/maximum (min/max) levels are established and utilized to drive inventory replenishment at depot and warehouse locations and McJunkin Red Man Corporation (MRC) periodically assesses the min/max levels for CDC depot locations, NiSource does not formally validate MRC's min/max changes. In addition, stockout reports are not reviewed by NiSource. Also, while the NIPSCO Operations team classifies and maintains certain inventory as emergency stock, adherence to defined emergency stock usage approval processes is inconsistent. NIPSCO personnel manage min/max levels for Indiana warehouse locations, but min/max levels are not periodically confirmed.	<u>Management Action Plan:</u> Supply Chain management and Engineering & Standards management will partner together to perform the following: • Perform an analysis across the entire company to evaluate the Company's inventory risk (December 2023) • Develop and execute a plan based upon the results of the inventory risk analysis to identify emergency stock and inventory components critical for ongoing operations across all material classes and all of the Company's operating areas, including considerations of how to acquire the appropriate emergency stock, emergency stock storage and handling procedures, validation of inventory levels for critical inventory components (including updates to min/max levels), applicable procedural adjustments, and validation of emergency stock and critical inventory component listings (the plan will be developed by February 2024; dates associated with specific action steps to be identified in the plan are to be determined) Supply Chain management will perform the following: • Identify the appropriate Operations management support necessary to partner with to complete the min/max action plans (December 2023) • Develop and implement a process to formally review/approve the MRC proposed min/max levels annually (April 2024) • Implement a process to verify that MRC has adjusted min/max levels within their system as agreed upon (April 2024) NIPSCO Warehouse Operations management will perform the following: • Implement a gatekeeping process to prevent the issuance of emergency stock unless approval is received (April 2024) • Formalize and implement a process to periodically review and confirm min/max levels (April 2024)

	<u>Responsible:</u> Dave Roy; VP of Supply Chain Eric Belle; VP of Engineering & Standards Jake Upper; Director of Fleet, Warehouse, Meter Operations and Emergency Management <u>Resolution Date:</u> Refer to the target remediation dates for each action item listed above.
<u>Evaluation Criteria:</u> Processes and controls are in place to ensure that the Company has identified and procured stock materials for usage in necessary activities, including in the event of an emergency and inventory components critical for ongoing operations; specifically: 1) a periodic evaluation is performed to assess the types and quantities of materials that are required to be on hand to establish min/max levels, including emergency stock and inventory components critical for ongoing operations; 2) the evaluation is documented and approved by the appropriate level of personnel; 3) the inventory system is appropriately updated to reflect adjusted min/max levels and is reviewed to ensure that the system levels agree to the approved min/max levels; 4) emergency stock materials are stored in a segregated location within the depots; 5) approval is required prior to the usage of materials identified as emergency stock; 6) periodic turnover requirements are established to ensure that the emergency stock materials do not become obsolete prior to usage; and 7) stockout alerts are established.	
2) <u>Inventory Accounting Controls (CDC and NIPSCO)</u>	Rating: 2
<u>Risk:</u> Potential that inventory account balance misstatements are not timely identified and resolved leading to a financial reporting misstatement.	
<u>Observation:</u> Inventory is not a material component of the Company's total assets and as a result, large inventory account reconciliation variances were not adequately reviewed, investigated, and resolved. Specifically, the NIPSCO and the Columbia Distribution Companies (CDC) materials and supplies inventory account balances in the General Ledger are not reconciled to associated subledgers or appropriate source information. In addition, the NIPSCO material and supplies inventory account reconciliations executed from September 2022 – April 2023 contained significant variances that were not investigated and resolved prior to the issuance of quarterly reporting. In 2023, the uninvestigated variance was as high as \$7.3 million (5% of the total account balance) with month-to-month variance swings as high as \$11.3 million and the variances were not communicated for inclusion within the consolidated quarterly variance analysis as required per the accounting reconciliation policy. Furthermore, controls to validate the completeness and accuracy of calculations for system average pricing in MAPPS (the NIPSCO inventory system of record) and the transfer of inventory activity data from MAPPS to PeopleSoft are not performed or included within the Sarbanes-Oxley (SOX) framework and testing procedures.	<u>Management Action Plan:</u> NIPSCO Accounting management, in conjunction with NIPSCO Warehouse Operations management, will develop and execute a plan to evaluate the control framework for NIPSCO materials and supplies inventory and determine necessary actions to address the identified risk. CDC Accounting management will identify and work with necessary parties to develop and execute a plan to evaluate the control framework for CDC materials and supplies inventory and determine necessary actions to address the identified risk. <u>Responsible:</u> Kevin Stanley, Controller Derek Ziolkowski, Controller Kristen King, Director of Consolidations, External Reporting, Technical Accounting & SOX Jake Upper; Director of Fleet, Warehouse, Meter Operations and Emergency Management <u>Resolution Date:</u> The plans will be developed by April 2024; dates associated with specific action steps to be identified in the plans are to be determined.

Evaluation Criteria:

Processes and controls are sufficient to ensure the Company's materials and supplies inventory balance is completely and accurately recorded within the financial statements; specifically: 1) key system functionality within the source systems has been identified and periodically reviewed; 2) data transfer from source system to general ledger is periodically tested to ensure data transferred is completed and accurately; and 3) a periodic reconciliation is performed (including variance review and investigation) and reviewed, comparing an independent source system sub-ledger report to the general ledger.

3) Invoice Accuracy Controls (CDC)

Rating: 2

Risk:

Potential that NiSource could be subject to pricing volatility and be overbilled for inventory purchases and activities, resulting in financial loss to the organization.

Observation:

For CDC, NiSource has delegated the duties of delivering and receipting inventory, as well as managing materials pricing data interfaced into NiSource's work management system (WMS), which occurs each quarter, to MRC. NiSource paid MRC \$83.5 million for materials and services delivered to CDC in 2022 and \$54.7 for materials and services delivered to CDC through August 2023.

Standard (firm) pricing is applied to materials ordered utilizing WMS, and associated invoices from MRC are automatically cleared for payment when MRC indicates that order fulfillment has occurred. While NiSource's business services partner, Tata Consultancy Services (TCS), is responsible for performing quarterly validation activities on pricing data in WMS, this control activity is insufficient to ensure the accuracy of payments to MRC. We evaluated a sample of invoices to verify the accuracy of pricing and analyzed the completeness of pricing information in WMS and identified the following:

- Pricing discrepancies between the price list in WMS and the invoice do not prevent invoice payment; for one invoice, the price invoiced by MRC and paid by NiSource was higher than the firm price agreed upon and maintained in WMS (\$33.88 vs. \$28.41)
- The standard (firm) price list in WMS is not always timely updated by MRC to include newly agreed upon pricing; we identified 22 items within WMS that did not have standard pricing for longer than one quarter, which is not in compliance with the service level agreement established with MRC
- Quotes to document pricing utilized outside of the standard (firm) pricing listing are not always obtained, approved and maintained; one (of three) quote for pricing not included in WMS was not provided

Furthermore, MRC is not always resolving NiSource-submitted receipting discrepancies (e.g., quantity ordered was not received, materials arrived damaged) timely and

Management Action Plan:

Supply Chain management will perform the following:

- Validate the completeness and accuracy of quarterly pricing updates within WMS during the review performed by TCS (April 2024)
- Implement a process to track, obtain and approve quotes for non-standard pricing used by MRC (April 2024)
- Develop and execute a plan to ensure the Company has visibility into pricing discrepancies identified and resolved by MRC (the plan will be developed by April 2024; dates associated with specific action steps to be identified in the plan are to be determined)
- Communicate expectations to operations personnel to identify receipting discrepancies upon delivery of materials into the depot locations by MRC (April 2024)
- Develop and execute a plan to communicate and enforce timely resolution of receipting issues reported to MRC by depot personnel (the plan will be developed by April 2024; dates associated with specific action steps to be identified in the plan are to be determined)

Responsible:

Dave Roy, VP of Supply Chain

Resolution Date:

Refer to the target remediation dates for each action item listed above.

there are no established service level agreement resolution timelines; of the 25 discrepancies submitted from January – September 2023, only one was resolved and 80% were aged over 60 days.

Evaluation Criteria:

Processes and controls are in place to ensure that NiSource has the appropriate oversight over invoicing to ensure that what we receive is what is being paid for; specifically: 1) there is established pricing validation for firm priced inventory items; 2) when inventory items are not firm priced, there is an established process to obtain pricing and validate that pricing against the invoiced amount; 3) prior to payment, there is system functionality in place to prevent payment for materials that have not been received; and 4) there is an established process to timely resolve pricing discrepancies.

4) Oversight of Inventory Availability (CDC)

Rating: 3

Risk:

Potential that a lack of physical inventory counts within the depot locations can lead to a lack of oversight of inventory movement within the depot locations as well as inaccurate financial reporting.

Observation:

MRC is contractually required to perform inventory counts at CDC depots (of both MRC- and CDC-owned inventory). NiSource does not ensure that required inventory counts occur and review count results. During our field visits to depot locations, we noted that materials ordered and allocated to capital projects are sometimes returned to CDC depots for utilization in future maintenance activities, but a process to record and track the quantity and location of these materials is not formalized, and NiSource does not have visibility to the quantity and locations of all materials physically on hand across the depot locations.

Management Action Plan:

Supply Chain management will perform the following:

- Identify the appropriate Operations management support necessary to partner with to complete the physical inventory count action plans
- Implement monitoring procedures to ensure MRC is performing contractually required periodic inventory counts of CDC depot locations
- Update inventory count process requirements established with MRC to include lost in construction inventory sitting in warehouses and depots

Responsible:

Dave Roy, VP of Supply Chain

Resolution Date:

The relevant Operations management support will be identified by December 2023. The remaining action plans will be completed by September 2024.

Evaluation Criteria:

Processes and controls are in place to ensure that NiSource has the appropriate oversight over inventory management activities executed by MRC; specifically: 1) roles and responsibilities between the vendor and Company employees/departments are defined and communicated; and 2) there is established monitoring in place to ensure activities performed by MRC are executed in line with Company expectations.

5) Key Performance Indicator Metrics (CDC and NIPSCO)

Rating: 3

Risk:

Potential that a lack of appropriately defined and communicated roles, responsibilities and expectations, along with the effective performance of critical vendor governance activities, can lead to ineffective management of key areas within the organization.

<u>Observation:</u> Although key performance metrics for MRC have been established within the vendor contract (e.g., on time delivery, order accuracy), NiSource does not perform validation procedures over the vendor-provided performance metric information to ensure that the information is complete and accurate.	<u>Management Action Plan:</u> A new contract with MRC was signed in 2023 that enhances key performance metrics reporting; Supply Chain management is currently in the process of reviewing and updating procedures to review the reported metrics. <u>Responsible:</u> Dave Roy, VP of Supply Chain <u>Resolution Date:</u> September 2024
<u>Evaluation Criteria:</u> Processes and controls are sufficient to ensure that vendor performance issues are identified and appropriately addressed; specifically: 1) roles and responsibilities for monitoring and metric validation are clearly defined and understood; 2) performance metrics are timely reviewed and instances of non-compliance are appropriately addressed and financial penalties are assessed and collected; 3) escalation processes associated with issue resolution are defined and understood; and 4) oversight activities are sufficient to ensure business process owners are effectively executing vendor performance management responsibilities.	
6) <u>Physical Security Access Controls (CDC and NIPSCO)</u>	
<u>Risk:</u> Potential that unauthorized and/or inappropriate physical access to facilities, including depot and warehouse locations, could result in security threats, asset misappropriation or damage, and negative impact to operations.	
<u>Observation:</u> While NiSource Corporate Security informally executes a practice to remove employee and contractor (including MRC employees responsible for inventory management) physical access to company facilities within 24 hours of termination, including access to depot and warehouse locations, this practice is not formalized and documented within company policy. As a result, access to facilities, including depot and warehouse locations, is not always timely removed. We performed limited, sample-based testing and identified some exceptions.	<u>Management Action Plan:</u> As the result of an internal audit of Data Center Operations performed in Q2 2023, Corporate Security performed the following: - Formalized and documented a process to review and remove physical access to all NiSource locations (including access to depot and warehouse locations) within 24 hours of termination and to obtain access badges at the time of termination within internal process documentation and the Corporate Security plans on the Company's intranet - Trained relevant associates on the updated requirements Corporate Security is also working with IT to determine if an IT solution can be implemented to automate the access removal process upon termination date. In addition, Corporate Security management will develop and execute a plan to sufficiently review and address the risk of inappropriate badge access within the depot and warehouse locations. <u>Responsible:</u> James Miller, Director Corporate Security

		<u>Resolution Date:</u> April 2024
<u>Evaluation Criteria:</u> Processes and controls are sufficient to ensure physical access to depot locations is restricted and monitored; specifically: 1) policies and procedures formally document a process to review and remove all physical access to NiSource locations within an established period of time after termination; 2) access listings are periodically reviewed and inappropriate access is timely removed; and 3) relevant associates are trained on the policy requirements.		
7) <u>Validation of Accuracy of Invoices (NIPSCO Only)</u>		Rating: 4
<u>Risk:</u> Potential that NiSource could be subject to pricing volatility and be overbilled for inventory purchases and activities, resulting in financial loss to the organization.		
<u>Observation:</u> NiSource paid MRC \$22.6 million for materials delivered to NIPSCO in 2022 and \$29.5 million for materials delivered to NIPSCO through August 2023. Pricing for materials purchased through Ariba from MRC can either be standard (firm) priced or agreed upon via a quote when firm pricing is not established (e.g., special order item, new material order). These quotes are not always obtained, approved and maintained, impairing NiSource's ability to validate the accuracy of invoices; one (of three) pricing quote requested by the audit team was not provided, and the related pricing was not included in the pricing list from MRC.		A management response is not requested; however, Internal Audit recommends that Supply Chain management implement a formal process to track, approve, and maintain quotes for non-standard pricing for materials purchased through Ariba utilized by MRC.
<u>Evaluation Criteria:</u> Processes and controls are in place to ensure that NiSource has the appropriate oversight over NIPSCO materials invoicing to ensure that what we receive is what is being paid for; specifically: 1) there is established pricing validation for firm priced inventory items; 2) when inventory items are not firm priced, there is an established process to obtain pricing and validate that pricing against the invoiced amount; 3) prior to payment, there is system functionality in place to prevent payment for materials that have not been received; and 4) there is an established process to timely resolve pricing discrepancies.		

COLUMBIA GAS OF PENNSYLVANIA, INC
53.53 III. BALANCE SHEET AND OPERATING STATEMENT
A. ALL UTILITIES

19. List extraordinary property losses as a separate item, not included in operating expenses or depreciation and amortization. Sufficient supporting data must be provided.

Response: Columbia Gas of Pennsylvania, Inc. has no extraordinary property losses.

COLUMBIA GAS OF PENNSYLVANIA, INC
53.53 III. BALANCE SHEET AND OPERATING STATEMENT
E. GAS UTILITIES

27. Submit a schedule for gas producing units retired or scheduled for retirements subsequent to the test year showing station, units, Mcf capacity, hours of operation during test year, net output produced and cents/Mcf of maintenance and fuel expenses.

Response:

None.