



PA PUC Audits How Does it Work

SEPTEMBER 9, 2026

NATHAN PAUL, MICHAEL FLYNN, AND EVAN BAKER

Normal Disclaimer Applies

- ▶ Auditors always have opinions and will usually let you know them. These opinions are our own and do not represent the position of the PUC, Commissioners, or anyone else at the Commission.

Bureau of Audits Mission Statement

The mission of the Pennsylvania Public Utility Commission's Bureau of Audits is to perform financial, management, operational, and specialized audits and reviews of certain regulated public utilities as legislatively mandated, required by tariff and/or directed by the Commission.

Two Divisions

4

Financial Audit:

- ▶ Adjustment Clause Audits
 - ▶ DSIC, Default Service, Smart Meter, etc.
- ▶ Tech Staff
- ▶ Special Projects

In July 2026, had 50 adjustment clause audit years in progress over 16 audits

Management Audit:

- ▶ Management & Operations Audit
- ▶ Management Efficiency Investigations
- ▶ Special investigations
- ▶ Other Projects

2 - 6 projects in process at any given time

Most audits are required by law (§1307d/e/f, §516, etc.) or directed by the Commission.

Why Audit

- ▶ The Law or Commission requires it!

But Why

- ▶ Checks and Balances in Government

No Really

- ▶ “In the field” verification of information thereby improving trust, accuracy, accountability, and performance of the auditee.

Where does it fit with the Commission



Information sharing –
before, after and
during audits with
advisory staff



Reports can be used
in formal
proceedings like rate
cases or
investigations



Independent review
provides some
confidence to the
public, Commission,
and other interested
parties



Fulfills Commission
mission statement to
“ensure safe and
reliable electric,...
service at
reasonable rates.”

Focusing in on Management Audits

- ▶ Required by Law
- ▶ Must occur every 5-8 years
- ▶ “... an examination of management effectiveness and operating efficiency.”
 - ▶ Our opinion that you can't do this without looking at the operations of a utility
- ▶ Management Audit is a holistic look at the utility including executive management, financial management, customer service, electric operations, and emergency preparedness to name a few

Summary – Electric Management Audits since 2022

Executive Management	Corporate Governance	Affiliated Interests	Financial Management	Electric Operations	Customer Service
10	2	16	11	18	16

Materials Management	Emergency Preparedness	Human Resources	Information Technology	Key Audit Matter
7	12	8	2	2

Electric Operations Focus vs Emergency Preparedness Focus

Electric Operations

Reliability	6
Overtime	4
CEMI	3
Storm Response	1
Damages	1
Training	1
Safety	1
Theft of Service	1
Total	18

Emergency Preparedness

Physical Deficiencies	3
Emergency Response Plans	3
Safety Equipment or Plans	3
Physical Security reviews	1
Business Continuity Plans	1
Cybersecurity Plan	1
Total	12

Reliability

Reliability Statistics



SAIFI, CAIDI, SAIDI,
CEMI, and MAIFI

Commission Benchmarks
and Standards
CEMI 10+
Excludable storms



Worsening Reliability



System Reliability Efforts



Outage Data

Vegetation
Equipment Failure
Animal
Vehicle

Reliability Spending

O&M Spending

- Budgeted vs. Actual Spending
- Budgeting Process

Capital Spending

- Capital Project Identification
- Project Prioritization
- LTIP and AAOP Review

Storm Readiness & Worst Performing Circuits

Storm Readiness

Storm Response and Restoration Plan

Storm Kits and Material Readiness

Dispatch and Response Times

Mutual Aid Agreements

After Action Reviews

Worst Performing Circuits

Worst Performing Circuit Identification

Circuit Reliability Improvement

Vegetation Management

- ▶ Tree Trimming Data
 - ▶ Overhead Line Data
 - ▶ Vegetation Management Spending
- ▶ Vegetation Management Programs
- ▶ QA/QC of Vegetation Management Efforts
- ▶ Vegetation Management Contracts

Asset Management

I&M Actual Results

Lifecycle Management

Smart Grid Initiatives

Pole and Line Inspections

Damage Prevention

Damage Prevention
Manual

One Call Participation

Infrastructure Damage
Data

Staffing and Management Systems

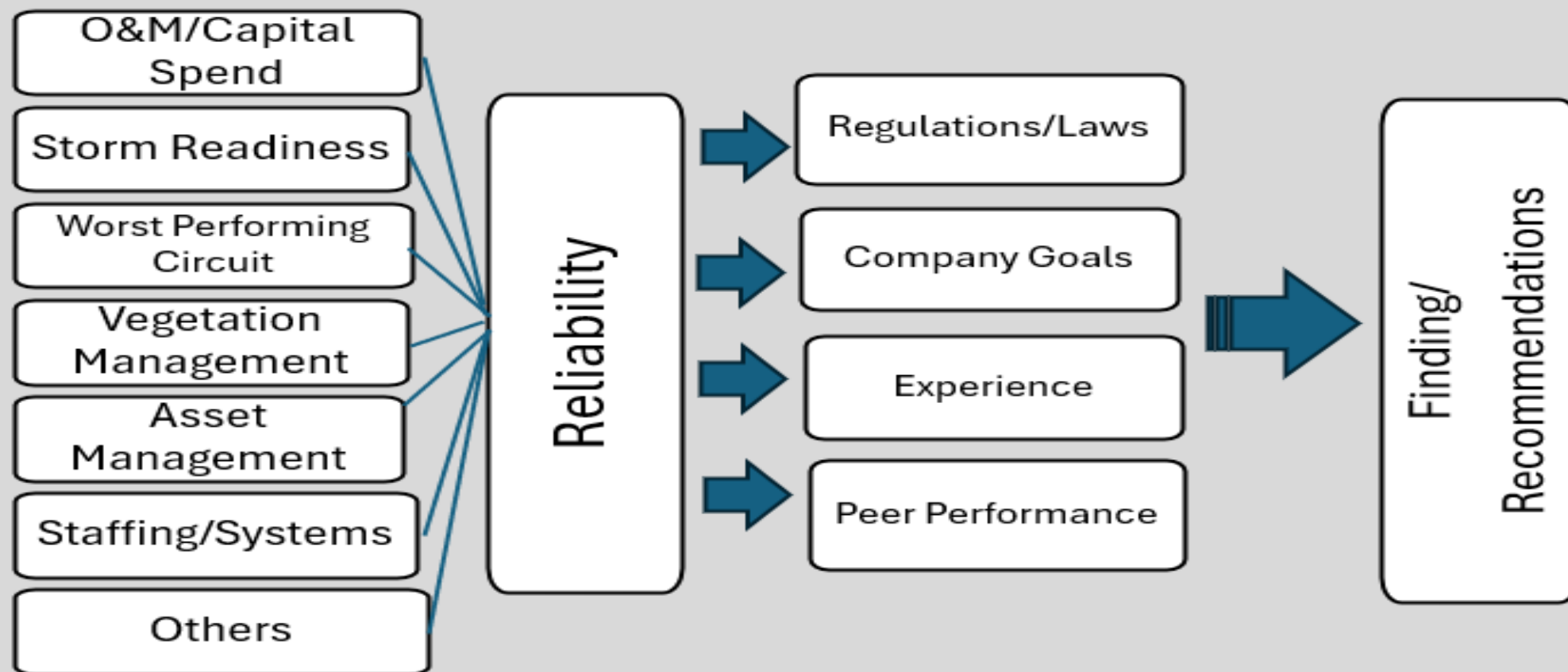
Staffing

- Staffing Levels
- Workforce Planning
- Training

Management Systems

- Work Management System
- Outage Management System

In a Nutshell



Emergency Preparedness Audit

A Note On CSI

- ▶ Confidential Security Information, or CSI, is protected under Act 156, The Public Utility Confidential Security Information Disclosure Protection Act.
 - ▶ This covers critical infrastructure and utility records that, if disclosed, could be used to commit a terrorist act or cause mass destruction.
 - ▶ These records are exempt from standard Right-To-Know Law requests.
 - ▶ These records are securely stored, only accessible by authorized people with specific training, and tracked individually.
 - ▶ Any public official or employee who knowingly or recklessly releases CSI commits a second-degree misdemeanor. This carries a fine up to \$5,000, up to one year in prison, and immediate job termination. If the information leak leads to damage to a utility, multiple felonies can apply.

Emergency
Preparedness
Audits are
comprised of
four main
subjects:

- ▶ Physical Security
- ▶ Cybersecurity
- ▶ Emergency Response
- ▶ Business Continuity

Physical Security Audit

- ▶ Review of the Physical Security Plan
 - ▶ How is it documented, reviewed, and tested?
- ▶ Review of risk analysis
- ▶ Identification of critical plant, equipment, and facilities
- ▶ Safety features.
- ▶ How is SCADA physically protected?
- ▶ How is the plan tested, and how often is this done?

Cybersecurity Audit

- ▶ Governance-focused, rather than technical details.
- ▶ Adapted from the NIST Cybersecurity Framework
- ▶ Review of cybersecurity policy and plan
 - ▶ How are they documented, reviewed, and tested?
- ▶ Interview of key personnel
- ▶ Review the utility's ability to identify, protect, detect, respond, and recover

Emergency Response Audit

- ▶ Review of the Emergency Response Plan
 - ▶ How is it documented, reviewed, and tested?
- ▶ Review of Risk Analysis
- ▶ Employee Emergency Response Training
- ▶ Communications Plan
- ▶ After Action Reviews

Business Continuity Audit

- ▶ Review of the Business Continuity Plan
 - ▶ How is it documented, reviewed, and tested?
- ▶ Processes for business recovery and resumption
- ▶ Backup of critical information, alliance or consortium agreements for recovery operations, emergency supplies
- ▶ Contingency planning.
- ▶ Employee training methodology, extent, frequency
- ▶ Drill Baby Drill!

Common Findings

- ▶ Finding: “Minor security and/or safety deficiencies were observed...”
 - Recommendation: “Correct minor security deficiencies at...”

- ▶ This is the most common Emergency Preparedness finding.
 - ▶ This will include things like:
 - ▶ Fence line issues related to wear and tear
 - ▶ Missing barbed wire at elevation differentials
 - ▶ Broken or misaligned door locks
 - ▶ Foliage overgrowing the fenceline or reducing visibility
 - ▶ etc.

Common Findings

- ▶ Finding: “First aid kits and fire extinguishers were not being inspected regularly.”
- ▶ Recommendation: “Develop an inspection program to ensure that all fire extinguishers and first aid kits are inspected and tagged monthly and resupplied as necessary.”
- ▶ Criteria:
 - ▶ NFPA 10 requires that fire extinguishers be inspected when they are put into service and at least monthly after that.
 - ▶ OSHA 1910.269(b)(3) requires first aid kit inspections at least annually.
 - ▶ While the standards do not specifically cover the documentation of inspection results, without documentation there is no way to prove compliance.
- ▶ The lack of a company-wide, centralized inspection program often leads to underequipped first aid kits or extinguishers that have not been inspected in a timely manner.

Common Findings

- ▶ Finding: “Security equipment is being replaced in an ad-hoc fashion.”
- ▶ Recommendation: “Develop a lifecycle tracking and replacement program for security equipment.”
- ▶ Criteria: It is a best practice to use a robust lifecycle management process to track security equipment patching, maintenance, and replacement needs.
- ▶ The lack of lifecycle management can lead to security equipment going without patching, upgrade, or replacement past its effective lifespan, leaving gaps in security.

Interesting Finding

- ▶ Finding: “The division of responsibilities for the physical security of SCADA and cyber equipment is unclear.”
- ▶ Recommendation: “Establish clear delineation of responsibility for the physical security of SCADA and cyber equipment.”
- ▶ Criteria: It is a best practice to be absolutely clear what specific party is responsible for the physical security of cyber assets, especially those related to SCADA systems.
- ▶ At some companies, the cybersecurity team assumes that the physical security team is responsible for all physical security, while the physical security team assumes that the cybersecurity team is responsible for the physical security of all cyber assets. This leads to neither team managing the security of those assets.
- ▶ A similar issue can be seen at some utilities where there was a recent merger, and security and/or cybersecurity has not yet been consolidated between the two parts of the new merged utility.



Questions?