Internal Controls Related to Identifying, Mitigating, and Preventing Recurrence of Noncompliance

Ed Kichline, Senior Counsel and Director of Enforcement Oversight
Leigh Faugust, CCEP, Enforcement Counsel

February 6, 2018

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Finding a problem, assessing the risk and cause of that problem, and addressing and preventing recurrence of that problem are key factors in establishing an effective compliance program.

Objectives

- Entity internal identification of noncompliance, prompt self-reporting, root cause analysis, mitigation/remediation activities.
- The impact of internal controls and mitigating activities on compliance monitoring and enforcement determinations.
- Case studies for Critical Infrastructure Protection (CIP) and Operations and Planning noncompliance.
- Available reference material such as User Guides and the NERC website.

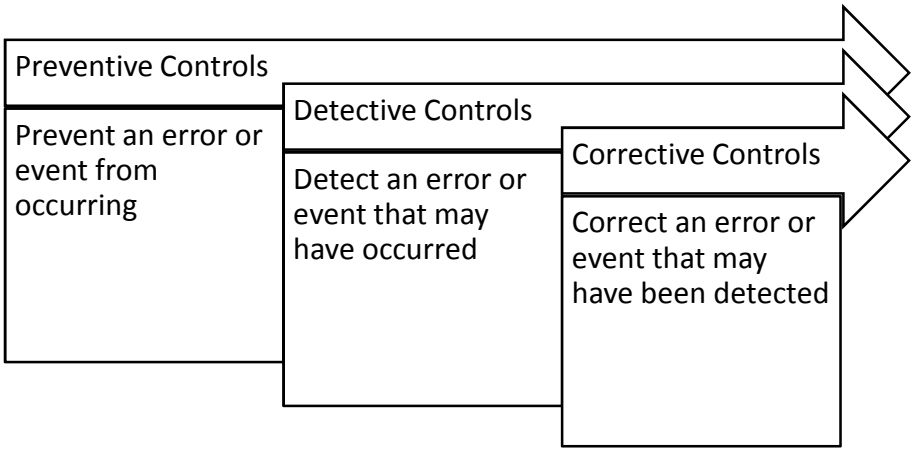
Mitigating Factors in Penalty Determinations: Self-Reporting

- Reporting by registered entity
  - Voluntary result of self-evaluation
  - Prior to audit notification
- Effect on penalty
  - Mitigating credit
    - Timeliness
    - Completeness
    - Repeat noncompliance

Mitigating Factors in Penalty Determinations: Corporate Culture

- Beliefs and behaviors that determine how a company's employees and management evidence a commitment to reliability of the bulk power system.
  - Presence and demonstrable quality of Internal Compliance Program
    - Identifying and addressing risk of noncompliance
  - Increasing internal communications related to reliability/security/compliance, prior to the noncompliance
  - Corporate reorganization to enhance reliability/security/compliance, prior to identification of the noncompliance
- Effect on penalty
  - Mitigating credit

Internal Controls



Root Cause

- What was the sequence of events that led to the issue?
- Why did the issue develop as it did?
- Is the sequence of events logical? Does it represent an accurate picture of what happened?
- Is this issue a symptom of a potentially larger problem?
- With respect to the cause of the noncompliance, were there extenuating circumstances?

Risk Assessment

Noncompliance may pose a wide spectrum of risks, ranging from inconsequential to catastrophic. The ERO Enterprise refers to risk posed to the reliability of the BPS as either **minimal, moderate, or serious**.

- Risk Evaluation
  - Facts/Circumstances
  - Mitigating Factors
  - Likelihood of Recurrence
  - Impact

Example: Critical Infrastructure Protection

- CIP-007 R2
  - Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.
    - R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.
    - R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).
    - R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

Managing Systems Security

- Factors that reduce risk
  - Preventive controls in place to prevent the unauthorized access to devices
  - Internal reviews to proactively identify noncompliance
  - Quarterly checks of access logs and patching records for verification
  - Correctly configured firewalls
  - Active monitoring of network traffic
  - Defense-in-depth system architecture
  - Strong process for authorizing access to shared accounts
- Factors that increase risk
  - Patching limited to only operating systems
  - Irregular review of logs
  - No tracking or changing of default passwords or generic accounts
  - No alerting for unsuccessful access attempts

Example: Operations & Planning

- PRC-005 R2
  - Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation or generator interconnection Facility Protection System shall provide documentation of its Protection System maintenance and testing program and the implementation of that program to its Regional Entity on request (within 30 calendar days). The documentation of the program implementation shall include:
    - R2.1. Evidence Protection System devices were maintained and tested within the defined intervals.
    - R2.2. Date each Protection System device was last tested/maintained

Maintaining Protection System Devices

- Factors that reduce risk
  - Redundant protection systems
  - Quarterly verification of maintenance and testing records
  - Periodic monitoring, inspections, and sampling of records
  - Alarms
  - Variable energy resources
  - Short duration for missed maintenance
  - Small size, remote location, or interconnection at lower voltage
- Factors that increase risk
  - Large percentage of missed devices
  - Long duration for missed maintenance
  - Irregular monitoring or inspections
  - Large size, central to load, or interconnection at higher voltage

Internal Compliance Controls

- Entity promptly self-reported vs. found at Audit.
- Instant noncompliance identified through proactive efforts that not only identified issues, but also included a root cause analysis to ensure that all noncompliances were identified, reported, and corrected.
- Cooperative throughout enforcement process.
- Quickly found and mitigated – short duration.

ICP Credit Considerations

- Did the compliance program find a problem that otherwise would not have been found?
- Did the compliance program include an extent of condition review?
- Did the compliance program include a root cause(s) analysis and find any other contributing factors?
- Was that assessment of the risk accurate, and does it take a holistic view of the entity and the circumstances of the violation?
- Is there a mitigation plan to address the problem?
- Does the plan include correction, detection, and prevention?
- Do the actions included in the plan address cause and risk?

Additional Resources

- Regional Entity representatives and case managers
- ERO Enterprise Self-Report User Guide
- ERO Enterprise Mitigation Plan User Guide
- Other Enforcement References
  - http://www.nerc.com/pa/comp/CE/Pages/Enforcement-and-Mitigation.aspx
  - http://www.nerc.com/pa/comp/Pages/Reliability-Assurance-Initiative.aspx

Questions and Answers