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

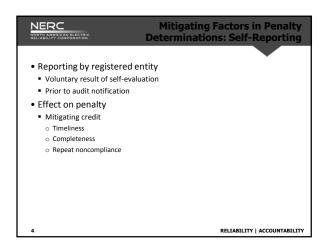
2

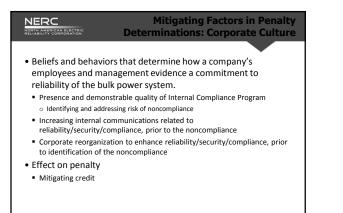
3

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.

RELIABILITY | ACCOUNTABILITY

NERC 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.

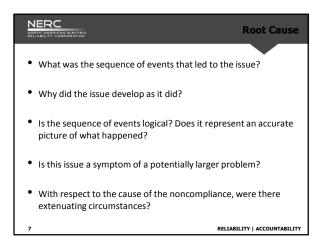




RELIABILITY	I	ACCOUNTABILITY

NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION		Internal Controls
Preventive Controls Prevent an error or event from occurring	Detective Controls Detect an error or event that may have occurred	Corrective Controls Correct an error or event that may have been detected
6		RELIABILITY ACCOUNTABILITY





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.

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

9

RELIABILITY | ACCOUNTABILITY

Example: Critical Infrastructure protections Protection

NERC 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

10

RELIABILITY | ACCOUNTABILITY

RELIABILITY | ACCOUNTABILITY

Example: Operations & Planning 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 program control of regram implementation shall include: o R2.1. Evidence Protection System devices were maintained and tested within the
- defined intervals.
- $\,\circ\,$ R2.2. Date each Protection System device was last tested/maintained

11

12

Maintaining Protection System Devices • Construction of maintenance and testing records • Cuarterly verification of maintenance and testing records • Quarterly verification of maintenance and testing records • Periodic monitoring, inspections, and sampling of records • Periodic monitoring, inspections, and sampling of records • Variable energy resources • Short duration for missed maintenance • Jactors 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

NERC 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.

RELIABILITY | ACCOUNTABILITY

NERC

13

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?

14

NERC

Additional Resources

RELIABILITY | ACCOUNTABILITY

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

15

