Internal Controls Evaluations
Better practices, Lessons Learned, and Industry Look Ahead

NPCC Compliance Workshop
May 23, 2018

Ben Eng
NPCC
Manager, Entity Risk Assessment
'Assuring BES Reliability through Risk and Controls Management'
NPCC Entity Risk Assessment

- Ben Eng, Manager – Entity Risk Assessment
- Duong Le – Sr. Compliance Engineer, ERA
- Lee Budd – Risk Consultant
- Mike Bilheimer – Sr. CIP Analyst
Purpose

• Controls “boot camp”
• Mentor on better practices to establish internal controls that are fully implemented
• Examples of Better ICE practices and documentation
• Industry Lookahead
Controls are Everywhere
Has this ever happened to you?

• Misplaced your keys, wallet, purse, smartphone?
• Forget the reason you walked back into a room?
• Lock yourself out of the house or car?
• Forget to do something?
• Forget to bring something with you?
• Dropped/Spilled something?
• Forget to renew something, pay a bill or mail a letter?
What were the causes for these mishaps?

- Distraction
- Multitasking/"Acrobatics"
- Haste
- Laziness/Inconvenience
- Complacency
- Overconfidence
- Variation of normal routine
- First time or seldom done activity
- Stubbornness/Refusal to use controls
What were the consequences?

• Minor annoyances/inconvenience
• Moderate impact
• Severe/Tragic
  – Feb 2015
What are these?

- Fire Sprinkler Head Components
- Firefighter
- Fire hydrant
- Smoke detector
- Fire extinguisher
- Fire buckets
- Please NO SMOKING
What Types of Risks Are There?

- Economic
- Health/Safety
- Property
- Occupational
- Transportation/Travel
- Operational/Business
Recognize These? Why?

- Mount Kilauea
- Harvey Weinstein, Kevin Spacey, Eric Schneiderman
- Matt Lauer, Al Franken, Mario Batali, Elizabeth Holmes
- Cambridge Analytica
- Romaine lettuce
- Wannacry
- Opiods
- Mark Zuckerberg
- E-cigarettes
- Dr David Dao
- ZTE phones
- Linked In
Risk

- **Risk appetite**: the amount and type of risk an organization is willing to accept in pursuit of its business objectives.

- **Risk tolerance**: the specific maximum risk that an organization is willing to take regarding each relevant risk.
“Control Silos” - Internal Control Designs

Internal Control Designs generally consist of a combination of the three “Control Silos” shown below:

- Document, review and assess Internal Controls that help you achieve your objective.
- “Tease out” and document controls that are taken for granted, or not formalized.
- Identify Key Controls.
- Ask the 5 “W” and 1 “H” questions pertaining to the control silos that are preventative, detective and/or corrective to “drift from compliance”.
- Interview Subject Matter Experts and task performers to determine how implementation of controls have been verified and monitored for effectiveness.
- Self-assess and obtain reasonable assurance that internal controls mitigate risks to BES reliability and meet compliance with specific NERC Reliability standards.
Effectiveness?
What are their control objectives?
Why the spikes?
Controls can degrade over time
Controls can literally degrade over “time”

What time is it?
Strengthening your Controls
Assessing your controls
Internal Controls

• Attributes of good controls design
  – Address Single Point of Failure
  – redundancy/alternate means to achieve objective
  – Confirmation of expected actions or timely response
  – Layering - Institute of Internal Auditors strongly suggests combination of all three types (P, D, C).
  – Enables consistency, repeatability, resiliency
  – Automation, early warning reminders
  – Frequent monitoring/shorter intervals
Assessment Criteria

- NPCC ICE team review of entity ICE worksheets and supporting documents
  - Offsite review (develop questions, actions for onsite walkthrough)
  - Onsite ICE walkthrough and interviews (“tease out” and document “unacknowledged/taken for granted” control designs)

Assessment Criteria
The CEA may use a binary effective/not effective method for assessing implementation effectiveness, or it may use a measured approach to assess internal control implementation. CEAs should have a documented methodology for assessing implementation, and this methodology may include, but is not limited to, the following:

- The automation of internal controls
- Compensating and supporting internal controls
- Registered entity identification of key controls
- The level of available internal control documentation
- Peer review of key controls within the registered entity
- Feedback on control design processes
- Registered entity’s internal review and testing of existing internal controls
This is what it’s all about
ICE Benefits

Expected benefits derived from a review of entity internal controls typically include the following:

• Enhanced attainment of BES reliability, Corporate Goals and Objectives;
• Greater alignment of staff performance to Key Performance Indicators;
• Improved operational performance (i.e., exceeding standards and requirements);
• Enhanced entity communication and interaction across organizational business functions;
• Targeted BES reliability risk-focused scoping;
• Possible reduction in audit duration;
• Improved risk and control awareness;
• Internal Control Design evaluation including:
  – Functional and Business Process Assessment;
  – Risk Identification, Mitigation & Remediation;
  – Design and Gap Analysis
  – Non-binding Recommendations for Internal Control Design Enhancement.
• Training/Succession Planning
• Resilience
• Progress toward High Reliability Organization
Controls vs Compliance

- Compliance with the requirement does not necessarily mean you have good controls for them – EOP-004, PRC-004, VAR-002, COM-002
- What is the purpose of controls? To mitigate the risks to reliability for the above.
- Documented controls and effectiveness testing/monitoring benefits:
  - Understanding of Key Reliability Functions
  - Training/Succession Planning
  - Resilience
  - Progress toward High Reliability Organization
Class Exercise

A. Introduction

1. Title: Geomagnetic Disturbance Operations
2. Number: EOP-010-1
3. Purpose: To mitigate the effects of geomagnetic disturbance (GMD) events by implementing Operating Plans, Processes, and Procedures.
4. Applicability:

4.1. Functional Entities:

4.1.1 Reliability Coordinator
4.1.2 Transmission Operator with a Transmission Operator Area that includes a power transformer with a high side wye-grounded winding with terminal voltage greater than 200 kV

5. Background:

Geomagnetic disturbance (GMD) events have the potential to adversely impact the reliable operation of interconnected transmission systems. During a GMD event, geomagnetically-induced currents (GIC) may cause transformer hot-spot heating or damage, loss of Reactive Power sources, increased Reactive Power demand, and Protection System Misoperation, the combination of which may result in voltage collapse and blackout.
Class Exercise – Control Objective

1. What is the control objective?

a) To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities.

b) To ensure that Facility Ratings used in the reliable planning and operation of the Bulk Electric System (BES) are determined based on technically sound principles.

c) To verify that the generator excitation control system or plant volt/var control function model (including the power system stabilizer model and the impedance compensator model) and the model parameters used in dynamic simulations accurately represent the generator excitation control system or plant volt/var control function behavior when assessing Bulk Electric System (BES) reliability.

d) To mitigate the effects of geomagnetic disturbance (GMD) events by implementing Operating Plans, Processes, and Procedures
1. Which could be the Risk Statement (for controls mitigation) for EOP-010

a) Risk to Reliability and operational continuity if a Responsible Entity fails to provide reportable events in a timely manner to ERO and other organizations in accordance with its Operating Plan.

b) Risk to Reliability and operational continuity if inaccurate Facility Ratings are used in the reliable planning and operation of the Bulk Electric System (BES). System Operating Limits and other limits may be impacted.

c) Risk to Reliability and operational continuity if the status (and changes) of the Generator Owner’s excitation control system is not made known to its Transmission Operator.

d) Risks to Reliability and operational continuity when the effects of geomagnetic disturbance (GMD) events have not been considered and addressed by developing and implementing Operating Plans, Processes, and Procedures.
1. What is the control objective? Where do you find it?

The Control Objective is the Purpose of the Standard “To mitigate the effects of geomagnetic disturbance (GMD) events by implementing Operating Plans, Processes, and Procedures”
[Answer: d ]

2. What are the Risks that the controls should mitigate?

The Risk statement can be developed by phrasing the Control Objective in the negative to identify the risks that controls could mitigate (specific to that standard/requirement)
[Answer: d ]
What should I do after I have identified, cataloged and assessed my controls?

- Document implementation testing
- Monitor effectiveness of control design
- Controls can be overridden or degrade over time
  - Control Designs are living and dynamic, not static
  - Apply Change Management
  - Has the control objective changed?
  - Have the Risks changed?
Examples - Better Practices

- Reliability Task Identification
- Internal Control Designs
- Address risks to reliability
- Link to April 2018 Webinar

Internal Controls for CIP and CyberSecurity

• Not a line by line review of controls specific to CIP Standard/Requirement
• Holistic approach following industry better practices.
• Center for Internet Security has refined and updated its Critical Security Control (CSC) Top 20
Internal Controls for CIP and CyberSecurity

• Corporate Risk Assessment methodology is suggested
• Goal is to have the entity self-assess and implement/improve controls for Reliability and Resilience
• See previous NPCC ERA Compliance Workshop presentations for CIP/Cybersecurity Controls

https://www.npcc.org/Compliance/Entity%20Risk%20Assessment/Forms/Public%20List.aspx
Closing Remarks

• Challenges to Reliability are prevalent
• Compliance may no longer be enough to be Reliable and Resilient
• Be proactive and self-aware of your control and risk mitigation designs that enable you to remain compliant with applicable NERC Reliability Standards.
• Internal Controls allow you to showcase where you surpass the requirements’ objective
Questions

Please email questions and/or feedback to ERA@npcc.org

More information available at NPCC ERA webpage

https://www.npcc.org/Compliance/Entity%20Risk%20Assessment/Forms/Public%20List.aspx

Thank you!!!