Compliance

Risk and Control

Preparing Energy Professionals for Tomorrow

NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

SOS Intl and NERC ID SOS_INTL_001 is recognized by the North American Electric Reliability Corporation as a continuing education provider who adheres to NERC Continuing Education Program Criteria

Course Objectives

Upon completion you will be able to:

- Explain performance audit objectives
- Understand NERC's vision for risk-based compliance
- Define internal controls
- Identify components of internal controls
- Explain the importance of good internal controls to identify, access, and correct deficiencies in compliance programs

2

Course Objectives

- Describe the use of a risk assessment for establishing internal controls
- Discuss utilizing a self-certification process to ensure continuous compliance
- Describe the benefits of incorporating compliance activities into work processes

3

Audit Experiences

- 0 tolerance approach
- Possible violations created equal
- One size fits all audits
- Administrative nightmare
- Backward looking – What's the value for Reliability
- Inconsistency across Regions

4

The NERC Vision
(NERC Standards & Compliance Workshop October 2012)

- **A sustainable model:**
  - Consolidated alignment of the Electric Reliability Organization (ERO) Enterprise
  - Industry cooperation to identify and mitigate risk
  - Reasonable administrative requirements
- **Strategically approaching risk:**
  - Base scope auditing and monitoring practices on risk in order to provide a reasonable level of assurance
  - Use a range of tools to prioritize and treat violations based on risk
  - Create distinctions in the application of compliance and enforcement given the risk to reliability

5

Generally Accepted Government Auditing Standards (GAGAS)

NERC Rules of Procedure, Appendix 4C (CMEP):

3.1 Compliance Audits

"…compliance audits are conducted on the registered entity's site to the extent required by NERC Rule of Procedure 403.11.2. Compliance audit processes for compliance audits conducted in the United States **shall be based on professional auditing standards recognized in the U.S., including (GAGAS) and standards sanctioned by the Institute of Internal Auditors"**

6

GAGAS

- Known as the Yellow Book
- Three types of audits
  - Financial statement audits
  - Attestation engagements
  - **Performance audits**

7

Performance Audits

These audits provide findings or conclusions based on an evaluation of sufficient, appropriate evidence against criteria.

Performance audits provide objective analysis to assist management and those charged with governance and oversight in using the information to:

- Improve program performance and operations
- Reduce costs
- Facilitate decision making by parties with responsibility to oversee or initiate corrective action

8

NERC 2013 CMEP

- Includes a set of reliability standards that were selected based upon ERO-identified high-risk priorities
- Incorporates a three-tiered approach to compliance auditing based on ERO-wide audit scope guidance
- Requires REs to consider a registered entity's actual and potential risk to the bulk power system (BPS) when determining the specific scope of each compliance monitoring activity

9

Compliance and Risk

- Risk
  - The possibility that something bad or unpleasant (such as an injury or a loss) will happen
- Risk Management
  - The process of evaluating the chance of loss or harm and then taking steps to combat the potential risk
- Risk Assessment
  - The process of risk analysis and risk evaluation
- Risk Treatment
  - The process of selecting and implementing measures to modify the risk

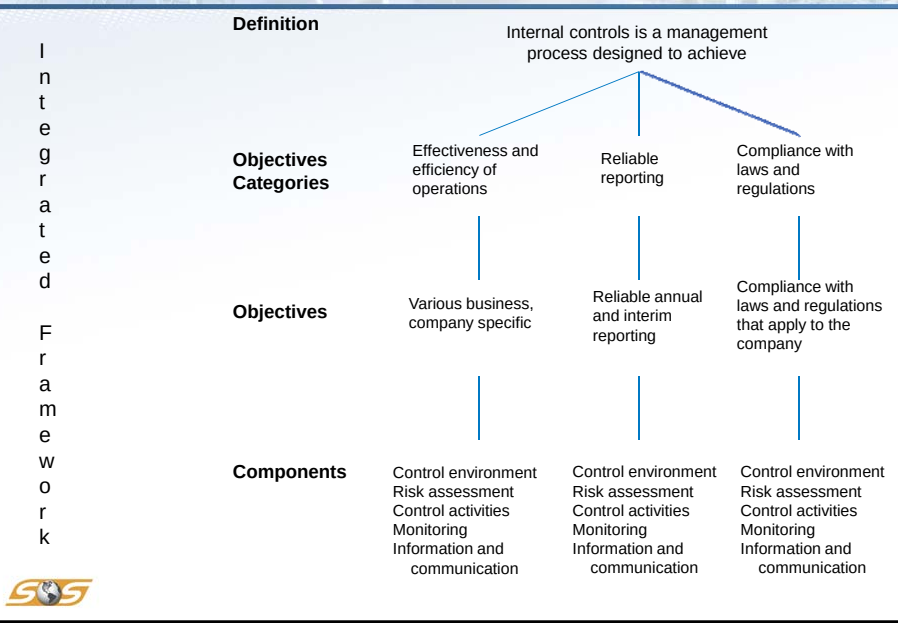
10

Managing Risk & Performance Audits
Internal Controls

- Internal Controls
  - Process designed to provide reasonable assurance regarding achievement of goals
- Major objectives of Internal Controls
  - Reliability and integrity of information
  - Compliance with policies, procedures, plans, laws, and regulations
  - The safeguarding of assets
  - The economical and efficient use of resources
  - The accomplishment of established objectives and goals

11

Internal Controls



Components

- Internal Controls Components
  - Control environment
  - Control procedures and processes
  - Monitoring
  - Information & communication
  - Risk assessment

13

Types

- Internal Controls Types
  - Detective controls are designed to detect errors or irregularities that may have occurred
  - Corrective controls are designed to correct errors or irregularities that have been detected
  - Preventive controls, on the other hand, are designed to keep errors and irregularities from occurring in the first place
- People are the key component of an Entity's internal controls
  - They establish the objectives, put controls in place, and operate them

14

Control Procedures

Control procedures are specific actions taken by organization's management and employees to ensure management directives are carried out.

- Performance reviews
- Segregation of duties
- Physical controls
- Information-processing controls

15

Evolution to Risk Based Compliance

- **Proposed COM-003-1**
  - R1 & R2 give more detailed communication protocol requirements for RC, BA, TOP, DP, & GOPs
- **R3 & R4**
  - Requires entities to implement a process for identifying deficiencies with adherence to the documented communication protocols specified in Requirement R1 & R2 that:
    - Identifies potential deficiencies,
    - Assesses the deficiencies found,
    - Corrects the deficiencies, and
    - Evaluates the process based on deficiencies found external to Part 4.1 and either
    - Implements modifications to the process when the evaluation determines that modification of the process is necessary to address the deficiencies found; or
    - Demonstrates that no modification to the process is necessary to address the deficiencies.

16

Process mapping

- Risk management tool
- Assist with defining processes and sub-processes
- Identifies stakeholders, customers, and owners
- Identifies control points
- Identifies control gaps

Process mapping

- Benefits
  - Employment involvement
  - A picture is worth a thousand words
  - Problem solving
  - Decision making
  - Big picture – impact
  - Best practices
  - Gaps
  - Training new employees
  - Audit presentation
  - **Integration of compliance in operations activities**

What now and why not now?

- Map processes
- Complete Risk Assessment
- Establish Internal Controls
  - Best practice for identifying and mitigating risk
  - Benefit of internal controls must be greater than cost to implement or maintain
- Utilize self-certification requirements and process as part of your internal controls program
  - Formalize self-certification process
  - Build internal controls into existing process

19

Future

- Internal Controls – It's a good thing!
  - Not just one more thing to do
- Risk based and performance based methodology
  - Not a one size fits all
  - Violations should be based on risk to reliability
- Focus on reliability
- In the present & looking forward– the **REAL** value for Reliability

20

Questions

21