Enabling internal controls programs and GRC technology to support NERC compliance

February 20, 2017

Your facilitation team

Manager
SDG&E, NERC Compliance Internal Controls Program Lead
Patrick Wells, CPA

Director
PwC, Midwest Power & Utilities Risk Assurance Regional Lead
Jake Stricker, CPA, CIA, CFE

Director
PwC, San Diego Power & Utilities Risk Assurance Lead
Tibyasa Matovu, MBA, CCEP

Manager
PwC, GRC Power & Utilities Technology Solutions
Andrew Gunter, JD
202 establishing internal controls programs to support NERC compliance

Course Objectives:
- NERC’s Reliability Assurance Initiative – Evolution and Impact
- Internal Controls Programs – Key Elements and Leading Practices
- GRC Technology Enablement – Archer, MetricStream, Assurx, Sigmaflow, Bwise
- Industry Insights – SDG&E

SDG&E journey:
- Strong historical compliance performance
- Embracing regulatory changes
- Increasing bench strength and technological capabilities
- Security viewed as a complex and key risk
- Greater assurance through internal controls program buildout

NERC’s Reliability Assurance Initiative (RAI)

Overview
- Multi-year effort involving NERC, Regional Entities and Industry
- Implement a more robust risk-based program for compliance monitoring and enforcement
- Compliance monitoring & enforcement must be “right-sized”
- Necessary for proper allocation of resources
- Encourages registered entities to enhance internal controls
- February 2015, FERC approved NERC’s proposed implementation of RAI

Impact
- An effective internal controls evaluation may:
  - Reduce scope of an audit
  - Alter compliance monitoring tools
  - Opportunity to develop strong risk and controls program
  - Provide greater assurance
  - Drive operational excellence
  - Reduce fines and penalties

Insights
- Having available resources with risk and controls knowledge is key but challenging
- Several utilities have started to:
  - Prioritize risks
  - Document controls
  - Establish test plans
  - Identify remediation activities
- Viewed as a multi-year effort
NERC Reliability Assurance Initiative Compliance Monitoring

Industry & Regional Risks | Company Specific Risks | Company Internal Controls | Tailored Oversight Plan
---|---|---|---
- Registered Entity Functions - ERC & Regional Characteristics - Events - RSC

**Input**

**Scoping**

**Inherent Risk Assessment**

**Internal Controls Evaluation**

**Focus**

**ICE**

Scoping and Focus for Entities not participating in ICE

**GMEP Tools**

**Entity Compliance Oversight Plan**

NERC compliance internal controls program elements

### Governance, monitoring and reporting
- Implement governance structure, tools and templates
- Implement ongoing QA/QC, monitoring and reporting mechanisms

### Risk assessment and planning
- Perform annual risk assessment identifying high risk processes, standards and requirements
- Determine ownership and schedule of controls program implementation activities

### Control design
- Review process documentation, RSAs, etc.
- Identify and document key risks and controls for high risk standards and requirements

### Control testing
- Develop testing requirements
- Conduct testing to assess the operational effectiveness of key controls

### Gap assessment + remediation
- Identify areas where controls do not adequately address standards and requirements
- Establish and implement action plans to eliminate gaps

### Training
- Provide risk and controls training to managers and SMEs responsible for implementing the controls program

### GRC technology enablement

---

PwC | Enabling internal controls programs and GRC technology to support NERC compliance
## Risk assessment summary

The identification, analysis and prioritization of relevant risks (uncertainties) to achieving NERC reliability and compliance objectives, establishing the basis for determining the nature timing and extent of controls and testing activities.

### External factors
- NERC Oversight Plan
- Regional Entity Oversight Plan
- Top 10 Highly Violated Standards
- Violation Risk Factor
- New/Revised Requirement
- Inactive Date

### Internal Factors
- Automation Level
- Lead SME Duration in Role
- Centralization of Process
- Process/Technology Change
- Process Maturity
- Compliance Date

### Audit results
- Self-Report/Log
- Reliability First Audit Finding

<table>
<thead>
<tr>
<th>High requirements</th>
<th>Medium requirements</th>
<th>Low requirements</th>
</tr>
</thead>
</table>

### Controls and Monitoring Activities - Future Considerations

### Develop risk and controls matrix

1. Procedures and RSAWs
   - Developed for each in-scope requirement
   - Documentation should be sufficient for third party to understand risks and controls

2. Risk control matrix
   - Map requirements, risks, controls, frequency, etc.

3. Conduct workshops/interviews and walkthroughs as needed
   - Validate results

### Consider Control Type
- Preventative vs. Detective
- Primary vs. Secondary
- Manual vs. Automated
- Entity Level vs. Direct
### Develop risk and controls matrix (continued)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Sub-requirement</th>
<th>Risk</th>
<th>Test Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP-004-0</td>
<td>R2, Part 1.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-004-1</td>
<td>R2, Part 1.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-004-2</td>
<td>R2, Part 1.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-004-3</td>
<td>R2, Part 1.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-004-4</td>
<td>R2, Part 1.1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Define test approach

**Develop test plan**

- A test plan is management’s plan for testing internal controls to prove operating effectiveness.
- Test plans should be reviewed and approved.

---

**Illustrative Example Only**

---

**More persuasive testing evidence**

= **Higher risk**

**Less persuasive testing evidence**

= **Lower risk**

---

PwC | Enabling internal controls programs and GRC technology to support NERC compliance 10
**Define test approach**

Nature of testing

- **Reperformance**
  - Provides highest level of assurance
  - Execute in same manner in which control was originally performed

- **Inspection/Examination**
  - Review of relevant documentation used in and that result from controls

- **Observation**
  - Observation of company’s operations and control performance
  - Use when no trail of evidence/documentation is available or observation of a pass/fail type of **automated control**

- **Inquiry**
  - Effective way to corroborate/follow up on evidence gained through other testing methods
  - Provides minimal level of assurance

**Develop and execute testing**

1. Develop test plan
   - Determine population and sample
   - Develop testing steps

2. Execute testing
   - Follow test plan to evaluate control
   - Use professional skepticism
   - Determine conclusions

3. Document test results
   - Complete all required fields in test plan
   - Follow established documentation standards
**Quality control**
Evaluate design and operating effectiveness

- Control deficiency exists when design or operation of a control does not allow management or personnel, in the normal course of performing their assigned functions, to timely prevent or detect operational or compliance issues
- Control deficiencies may be identified at any stage of the assessment process

<table>
<thead>
<tr>
<th>Deficiency in design</th>
<th>Deficiency in operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>• An existing control is not properly designed so that, even if control operates as designed, the control objective would not be met (i.e., fail to prevent or detect reliability issue or non-compliance)</td>
<td>• Properly designed control does not operate as designed</td>
</tr>
<tr>
<td>• Deficiency in design is identified during documentation and quality reviews</td>
<td>• Person performing control does not possess necessary authority or competence to perform control effectively</td>
</tr>
<tr>
<td></td>
<td>• Deficiency in operation is normally identified during testing of key control activities, but may also be detected during test of one transaction during walkthroughs or during a quality review</td>
</tr>
</tbody>
</table>

**NERC control framework challenges**

Reliance on spreadsheets, shared folders, and SharePoint solve the immediate documentation need, but creates its own challenges, including:
- Maintenance of Controls
- Reliance on Manual Workflow
- Execution of Control Tests
- Relating Control Tests, Evidence, Risks, and Findings to Controls
- Monitoring of Corrective Action Plans
- Reporting
**Leveraging technology effectively**

*Benefits achieved by companies who have implemented GRC technology:*

- Improved monitoring: 83%
- Enhanced reporting: 83%
- Automation driving more efficient workflow: 83%
- Reduction in errors by eliminating manual processes: 67%
- Elimination of redundant systems: 67%
- Expanded access to centralized data: 67%
- More timely decision making: 33%

The results provided above include only those companies that have implemented a non-ERP based GRC technology (e.g., Archer, MetricStream, BWise, etc.).

*PwC Power & Utilities State of Risk Survey*

**Processes/Technology solutions are siloed**

Companies often support their siloed Risk and Compliance processes approach with siloed technologies. This results in inefficiency, reduced effectiveness, duplication of effort and lack of transparency.
**Aligning GRC efforts**

<table>
<thead>
<tr>
<th>Foundational components</th>
<th>Core GRC principles</th>
<th>Analysis &amp; reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Language</td>
<td>Objectives setting</td>
<td>Data Aggregation</td>
</tr>
<tr>
<td>Common Organizational View</td>
<td>Risk appetite &amp; tolerance</td>
<td>Data Analysis</td>
</tr>
<tr>
<td>Methodologies</td>
<td>Policies &amp; standards</td>
<td>Data Presentation</td>
</tr>
<tr>
<td></td>
<td>Risk &amp; control assessment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issues management &amp; remediation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Monitoring</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Testing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reporting &amp; analysis</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Communication &amp; training</td>
<td></td>
</tr>
</tbody>
</table>

**Technology-driven monitoring and testing creates sustainability**

Dashboards enable Executive Leadership and Management to track NERC risks and related controls. As well as create a Global Dashboard to consolidate Risks and Controls across the enterprise.
Thank you for your participation!