Internal Controls and Critical Infrastructure Protection (CIP)

July 25, 2013

Steven Keller
skeller.re@spp.org

Helping our members work together to keep the lights on... today and in the future
Why Internal Controls?

• Effective Internal Controls help you achieve compliance with NERC Standards
• Internal Controls are already used by many entities for compliance with Sarbanes-Oxley, public financial reporting, DOE compliance
• Internal Controls are reviewed during pre-audit review
• Internal Controls are reviewed during a CIP Audit for compliance with NERC standards and requirements
Even more to keep up with???
Culture of Compliance

• We already look at your internal controls
  - Pre-audit survey
  - Culture of compliance questions
  - CIP audit
Internal Control is a Process

- It is a process with an objective to reduce risk
- Entity needs to define its own internal controls
- No a “one size fits all”
- Needs officer or other senior manager oversight
Reasonable Assurance

- **What is Reasonable Assurance?**
  - Auditor must decide, exercising professional judgment, whether evidence available within limits of time and cost is sufficient to justify an opinion
  - An internal control, no matter how well designed and operated, cannot guarantee an entity’s objectives will be met because of inherent limitations in all internal control systems
What are Internal Controls

• Broad definition:
  – Accounting procedure or system designed to promote efficiency or assure implementation of a policy, safeguard assets, or avoid fraud and error

• Five interrelated components:
  1. Control environment
  2. Risk assessment
  3. Control activities
  4. Information and communication
  5. Monitoring

[Diagram: Five interrelated components of internal controls]

coso.org
Where do we find objectives?

• Look at CIP requirements
  – What are they asking?
  – What does the requirement say?
    ▪ CIP-007-5 R1 (Enabled Ports)
    ▪ CIP-003-3 R2 (Assignment of Senior Manager)
    ▪ CIP-007-5 R2 (Patch Management)
Example 1

- **CIP-004-3 R2 and PER-005-1**
  - Entity must have at least an annual training (12 months) for personnel unescorted access to CCA.
  - Or at least every 12 months for RC, BA and TOP provide their System Operators with 32 hours of emergency training.
  - In a nutshell: Training is required for most personnel with access to NERC-related information or computers.
  - What are some possible common controls?
Example 2

• **CIP-003-5 R1**
  - All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined Electronic Security Perimeter (ESP)

• **Possible Entity Internal Controls:**
  - Checklist that’s followed when adding a new applicable Cyber Asset(s) to ESP
  - Yearly physical inspection and count of all applicable Cyber Assets connected to ESP
CIP AND RISK
Understanding and Managing Risk

• Where is risk and what is the best way to manage it to an acceptable level?
• How do we provide reasonable assurance that objectives will be met?
• CIP auditors want reasonable assurance that requirement’s objectives are met
Example risks in CIP World

- Patch or a virus definition crashes your system
- Visitor walks unescorted in your control room
- Quarterly access reviews are not completed
- BES Cyber Asset gets taken out of a data center without data being wiped
Risk Analysis

- Assess likelihood (frequency) of risk occurring
- Estimate potential impact if risk were to occur
  - Consider quantitative and qualitative costs
- Determine how risk should be managed
Measuring risk

- Frequency/likelihood
- Cost
- VRF Impact
  - High
  - Medium
  - Low
Risk Response

• **Avoidance** – Not participating in events that give rise to risk
  – **Example** – Not intermingling corporate assets with CIP assets

• **Acceptance** – No action taken
  – **Example** – FERC does not approve of acceptance of Risk, per Order 706
Risk Response

• **Reduction** – Specific actions taken to reduce likelihood or impact or both
  
  – **Example** – Provide CIP Training on BES Cyber Systems to all employees

• **Sharing Risk** – Reducing likelihood or impact by sharing portion of risk or shared responsibility
  
  – **Example** – Violation that impacts multiple people. Training helps reduce this risk by teaching staff about consequences and prevention.
CONTROL ACTIVITIES
What is a Control Activity?

- Process to help organization accomplish specific goals or objectives by mitigating risk
- Effective controls are ...
  - Complete
  - Accurate
  - Valid
  - Timely
  - Simple
  - Practical
  - Reliable
  - Cost-effective
Type of Internal Controls

1. Preventive

2. Detective

3. Corrective
Control Types: Preventive

- Designed to avoid unintended event or result at the time of initial occurrence (such as blackout)
- Prevents errors
- Proactive approach
- Often includes approvals/authorizations
Preventive Examples

• **Camera**
  – Remote access control to PSP

• **Anti-virus/anti-malware software**
  – Prevent data loss

• **Password and PIN numbers**
  – Prevent unauthorized access
Control Types: Detective

• Designed to discover an unintended event or result
  – After initial processing has occurred
  – Before the ultimate objective has concluded

• Reconciliations
  – Personnel approving or executing transactions should not perform reconciliations

• Reviews

• Manual or Automated
Detective Examples:

- After you change your password, vendor sends you a notification email
  - Detect unauthorized access to account
- Quarterly Access Reviews
  - Detect errors
- Audit trails
  - Who did what and when
Control Types: Corrective

- Designed to correct errors or irregularities that have been detected
Corrective Examples

• Backup tapes

• System Rebuild procedures

• Incident Response procedures
Complimentary Controls - Access Logging

• **Control Objective:**
  - No tail-gating

• **Preventive:**
  – Every employee who badges in a data center must also badge out of the data center

• **Detective:**
  - Manual weekly review of logs

• **Corrective:**
  - Training
What are control activities good for?

• Reducing mistakes and accidents
• Compliance
• Management tool to quickly review that work is being completed as expected
• Identifying training needs (trending)
• Audits
Control Activities: Physical

- Equipment, inventories, BES Cyber Assets, other assets are:
  - Secured physically
  - Periodically counted

- Examples:
  - Door badge readers
  - Cameras
  - Visitor Management
  - Alarms
Control Activities: Data

• How do you protect the CIP data?
  – Population
  – Updates
  – Accuracy
  – Completeness
  – Validity

• Examples:
  – Controlling file access
  – Training employees
  – Reviewing data access
Control Activities: Supervisory

• Assess whether other transaction control activities are being performed:
  – Completely
  – Accurately
  – According to policy and procedures

• Can be a high-level review or a more detailed review

• Examples:
  – Review manual changes completed by staff
  – Review if all steps in a process have been completed accurately and timely
  – Approve timesheets, vacation requests, etc.
Elements of a Control Activity

- **What**
  - Develop brief, concise description of what is done

- **Who**
  - Use titles – not names
  - And designee

- **Frequency**
  - For each operating day, for each week, etc.

- **Documentation/Evidence**
  - What is it, where is it, who gets it, how is it accessed, how is it backed up
Example CIP-009-5 Control

• **Objective**
  – Test Recovery Plan for BES Cyber Systems

• **Control Type**
  - Preventive and Detective

• **Control Activity**
  - Supervisory

• **Risk**
  - The recovery plan will fail when needed

• **Risk Measurement**
  – Likelihood of plan failure

• **Risk Response**
  – Reduction

• **Who**
  – Use titles – not names
  – List responsibilities of titles

• **Evidence**
  – Recovery Plan
  – Evidence of recovery plan test

• **Frequency**
  – Test every 15 months
Example CIP-004-5 R3 Control

• **Objective**
  – Perform Personnel Risk Assessments (PRA)

• **Control Type**
  - Preventive

• **Control Activity**
  - Supervisory

• **Risk**
  - Unauthorized access to PSPs and BES Cyber Systems

• **Risk Response**
  – Reduction

• **Risk Measurement**
  – Likelihood of someone having access to something they should not

• **Who**
  – Employees with access to BES Cyber Assets

• **Documentation**
  – Documents showing PRA completion within the specified time frame

• **Frequency**
  – Initial, then every 7 years
Effectiveness and Efficiency of Controls

• Test controls to verify there are no material weaknesses or significant deficiencies
  - Do not test your own controls!

• Management should confirm control activities are carried out in a timely manner
Things to Remember

• Identify Objectives
• Identify Risks
  – What can make this go wrong....
• Develop/Document Controls
• Test Controls
SPP RE Training Videos: vimeopro.com/sppre/basics

- Audits: Top 10 Ways to Prepare
- CIP Audit: What to Expect
- CIP-005: Electronic Security Perimeter
- CIP-005-3 R3
- CIP-006: Physical Security
- CIP-007 Compliance
- CIP-007: R1 System Configuration
- CIP-007 R3 and R4
- Compliance Education at My Company
- Internal Compliance Programs Q&A
- Event Analysis-Entity Perspective
- Evidence Submission
- Firewalls: 13 Ways to Break Through
- Hashing: How To
- Human Performance - Entity Perspective
- Human Performance - NERC
- Mitigation Plans: Milestones, Completion, and Evidence
- Mock 693 Audit
- Self-Reporting: When and How
- TFE Expectations and Issues
- Training Employees on Compliance