Internal Controls
A Practical View

Compliance Spring Workshop
May 9 -10, 2017
Objective

To provide FRCC entities with a practical understanding of Internal Controls
Definition of Internal Controls

Processes, practices, policies or procedures, system applications and technology tools, and skilled human capital an entity employs to prevent, detect, and correct noncompliances with Reliability Standards and/or address risks associated with the reliable operation of its business*

*ERO Enterprise Guide for Internal Controls December 2016, pg. 10, NERC.
Definition of Internal Controls

Examples of internal controls may include:
Oversight, risk assessment, control activities, communications and training and monitoring

Internal controls operate at both an entity or organizational level, as well as, an activity or process level*

*ERO Enterprise Guide for Internal Controls December 2016, pg. 10, NERC.
NERC has endorsed the usage of internal controls amongst its entities and organizations as a method to provide assurance of compliance with NERC Reliability Standards.

In its 2016 ERO Enterprise Guide for Compliance Monitoring, NERC announced:

“A good sound business approach to incorporating effectively designed and implemented internal control improves operational and compliance performance. Through evaluations, the CEA [Compliance Enforcement Authority] may take into account good governance practices of registered entities that effectively manage risk to BPS.”

Why We Endorse Internal Controls

Internal Controls Truism #1
A process equipped with a well designed internal control, will greatly increase the probability of the process completing the desired goal.

Applying additional well designed internal controls to the same process will improve the chances of completing its goal, and will help add sustainability to the control.
Why We Endorse Internal Controls

Internal Controls Truism #2

We all use internal controls
   We may not recognize them
   But we all use internal controls
   Why, because they work
Automotive Safety Devices/Controls

- **Anti-lock braking system (ABS)** prevents the wheels from locking up (ceasing rotation) and thus avoiding uncontrolled skidding.
- **Lane departure warning systems** alert the driver of an unintended departure from the intended lane of travel.
- **Vehicle backup cameras** that alert drivers to difficult-to-see objects in their path when reversing.
- **Traction control systems** which restore traction if driven wheels begin to spin.
- **Tire pressure monitoring systems** or **Deflation Detection Systems**
- **Adaptive cruise control** which maintains a safe distance from the vehicle in front.
## Controls as a Process Improvement

<table>
<thead>
<tr>
<th>Goal/Objective</th>
<th>Standard Process</th>
<th>Process Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stopping and Slowing the Car Safely</td>
<td>Automobile Braking System</td>
<td>Anti-Lock Brakes</td>
</tr>
<tr>
<td>Minimize Blind-Spot Related Collisions While Driving</td>
<td>Driving and Parking a Car</td>
<td>Collision Avoidance Systems, Backup Cameras</td>
</tr>
<tr>
<td>Drive safely on wet or slippery road surfaces</td>
<td>Front Wheel Drive Rear Wheel Drive All Wheel Drive</td>
<td>Traction control systems</td>
</tr>
</tbody>
</table>
Compliance Internal Controls

• **Automated alerts or notification systems** that alerts an entity’s cyber security personnel, at least once every 35 days, regarding the evaluation of a new security patch (CIP-007-6 R2.2)

• **Peer reviews** to verify that equipment testing and maintenance is completed as required (PRC-005-1.1b R2)

• **Automating a process to auto-disable cyber access** for cyber credentialed employees that have not completed training by the due date (CIP-004-6 R2.2, 2.3)
Types of Internal Controls

- Preventative: ✓ Before
- Detective: ✓ During
- Corrective: ✓ After
Internal Controls Characteristics

- Preventative – Proactive, before something happens; Normally authorized and approved procedures; Training

- Detective - Finds errors or irregularities; EMS System alarms; Independent review of operating performances; Reconciliations

- Corrective - Assess instances of noncompliance and return an activity to a state of compliance; Requires making adjustments after discovery; Procedural; Restoration Plan; Root Cause Analysis Process
Preventative Internal Controls

Preventative – Designed to discourage noncompliance with the Reliability Standards

Proactive internal control that help ensure management’s objective of achieving compliance with Reliability Standards

Example: Documented process that requires a training schedule be developed and maintained that includes all required training and the scheduling of training to ensure it is completed prior to the dates required by the applicable Reliability Standard requirements
Preventative Controls Examples

A standard requiring training prior to receiving access to BES Cyber Systems

Controls may include:
• Computer program that notifies individuals of training deadlines and due dates
• Computer program alerts management of individuals that are about to lose access due to training expiration

While the standard requires training, the control is the tool or process that ensures that the training occurs
Detective Internal Controls

Detective – Designed to find errors or irregularities and support effective compliance

Documented process that requires a periodic review conducted to identify required training that was not completed as scheduled and training that was not completed per the Reliability Standard requirements

An example would be a quarterly review of completed training records to identify individuals that have not completed training by the required deadline
Detective Controls Examples

A standard requires defined inspection schedules, or maintenance activities.

Detective controls could include:

• A computer system that conducts a quarterly review of completed training records to identify individuals that have not completed training by the required deadline

• A procedure that schedules inspections twice annually, while the standard only requires an annual inspection

The standard defines the inspection requirements, the control is the tool or process that ensures that the inspections occurs and meets the requirement.
Corrective Internal Controls

Corrective: Designed to assess instances of noncompliance and return an activity to a state of compliance.

Example: Automatic Voltage Regulator (AVR) status indication alarm

- Alarms in the Transmission Operator’s Control Center indicating an AVR status change from Automatic to Manual
- Provides notification to the TOP of an AVR status change within 30 minutes as required by Reliability Standard VAR-002

The standard AVR reporting requirements, the control is the tool or process that ensures that the reporting of AVR status occurs, and meets the requirement.
Audits and Internal Controls

Current Monitoring Processes:

Reliability Standards tell us **what** is required

The Entity describes **how** they comply with the requirement via the RSAW response

**New - Controls Review:** Auditor asks entity what additional **processes** are in place that ensures compliance with applicable requirements occurs
Monitoring and Controls Scenario #1

FAC-003-4  R6 Vegetation Management

Requirement: Perform a Vegetation Inspection of 100% of its applicable transmission lines, at least once per calendar year and with no more than 18 calendar months between inspections on the same ROW
Audit Scenario #1

FAC-003-4  R6 Vegetation Management

Expected Entity Deliverables:

• Provide a procedure that describes processes related to how your entity performs its Vegetation Inspections

• Provide a schedule for inspections that ensures 100% of its applicable transmission occurs at least once per calendar year and with no more than 18 calendar months between inspections on the same ROW

• Provide a checklist that includes a sign-off signatures by the entity’s inspectors
Controls Interview Scenario #1

FAC-003-4  R6 Vegetation Management

Possible Review Enquiries:
What actions or tools (controls) do you employ to reasonably assure compliance with this requirement?

Possible Responses:
• Scheduling software that sends out email notices or alerts when vegetation inspections are due
• Documented process in place that requires a signed independent verification that inspections have occurred
• Training provided for workers designated to conduct vegetation inspections
Internal Controls Summary

Controls:

- Can be plans, peer/independent/management reviews, system applications and technology tools

- Often appears as an EMS system, automated alarms or alerts, automated notifications

- Should be documented in entities procedures, plans, or processes

- Provide reasonable assurance that an objective/goal will be successful
Questions?

Orlando Brandon
obrandon@frcc.com
(813) 609-4778