Get Control of Yourself!

By: Denise Hunter, Principal Technical Auditor

Welcome to the first in a series of articles focusing on developing a strong internal control program. Our goal with this column is to share information, suggestions, and industry examples to aid in understanding what an internal control program consists of, thus providing insight on how to craft a control program and suggestions to help strengthen existing programs.

An internal control program consists of five components:

- Culture
- Risk Assessment
- Internal Control Activities
- Information and Communication
- Monitoring

Over the last few years, RF has offered ideas regarding possible approaches to addressing the internal control activity components and understanding what an internal control activity is and how to document it. To advance our conversation regarding the internal control program, we now will explore the component of identifying risk and determining appropriate, feasible mitigating control activities.

There are numerous factors that need consideration to properly assess an entity's risk to the BES: organizational structure, compliance history, registration, ERO/RF risk elements, to name a few. The majority of these criteria are unique to the entity, and therefore would be difficult to discuss in a generalized fashion.

The exception is the ERO/RF risk elements. NERC identifies risk elements using data including, but not limited to:

- compliance findings;
- event analysis experience;
- data analysis; and
- the expert judgment of NERC and Regional staff, committees, and subcommittees (e.g., NERC Reliability Issues Steering Committee).[1]

During the 2019 CMEP IP process the ERO identified eight ERO risk elements. RF identified four additional risk elements and expanded on one of the ERO risk elements.

Over the course of the next few newsletters, this series will review the eight risk elements, aiming to provide applicable Standards, industry risk examples and relevant mitigating controls, with detailed insight into one suitable mitigating control for each risk element.

We begin our review with **Improper Management of Employee and Insider Access**. The focus of this risk element is the risk posed by the *human element of security*. Regardless of the sophistication of a security system, there is potential for human error. Entities must identify and manage the risk of how many people have access, both physical and technical, and be aware of the complexity of the tasks employees are asked to perform.

When considering this element during risk assessment, at a minimum, forethought should be given to:

a) Structural access during position changes, terminations, organizational changes, etc.

b) CIP systems and technology access, as outlined within the CIP Standards,

c) computerized spreadsheets and workbooks utilized to perform complex tasks, and

d) all computer systems used to maintain a reliable grid.

The following Standards have been identified as applicable to this risk element:

- Personnel & Training (CIP-005-5)
- Electronic Security Perimeter(s) (CIP-004-6)
- Physical Security of BES Cyber Systems (CIP-006-6)
- System Security Management (CIP-007-6)
- Configuration Change Management
- Vulnerability Assessments (CIP-010-2)
- Information Protection (CIP-011-2)

[1] 2019 ERO CMEP Implementation Plan V2 November 2018, page 7

2019 Risk Elements

Improper Management of Employee and Insider Access
Insufficient Long-Term Planning Due to Inadequate Models
Insufficient Operational Planning Due to Inadequate Models
Spare Equipment with Extended Lead Time
Inadequate Real-time Analysis During Tool and Data Outages
Improver Determination of Misoperations
Inhibited Ability to Ride Through Events
Gaps in Program Execution

Continued on page 13

Get Control of Yourself!

Continued from page 12

However, I feel the risk elements often permeate more than the identified Standards, applying to all areas of the organization.

The CIP Standards noted above focus on incidents regarding security breaches, either physical or technical, and securing cyber information. Ensuring the security of those areas is of the utmost importance, however the risk identified by this element should expand beyond those to areas such as excel workbooks designed to perform complex tasks used for Grid reliability.

A few examples: Facility Ratings (FAC-008-3), Transmission Relay Loadability (PRC-023-4), Generator Relay Loadability (PRC-025-2). Often times excel workbooks are used to ensure consistency while performing these calculations, however access to the workbook, and actual cell calculation information, is not protected.

These workbooks should be:

1) Owned by one position within the department responsible for the function, thereby ensuring only approved changes are implemented,

2) password protected, allowing access to only those personnel that are performing that function, and

3) locked so that cells within the workbook containing 'static' information (i.e. calculations) can't be overwritten.

The final step in addressing the risk elements is to identify the appropriate internal control activities to mitigate the risk. There are a number of internal controls that should be considered when crafting a control activity to mitigate this risk: Access controls, Asset Management controls, Change Management controls, Termination controls, and Segregation of Duties.

The objective and activities (to the right) can assist in crafting a strong Access Control. With the addition of each activity listed above, the breadth and strength of the control increases.

A 'perfect' internal control will never exist, however by identifying the appropriate access levels, and including activities within the control that address personnel movement, the risk of Improper Management of Employees and Insider Access can be mitigated.

This newsletter will be captured on the Internal Controls Knowledge Center, and if you have any questions or areas of an internal control program that you would like answered or addressed, the Knowledge Center contains a link for those submissions.

I look forward to continuing this conversation in upcoming newsletters.

Access Controls

Objective:

The selective restriction of access to a place or other resource.

Control Activities:

Including the following activities will help to strengthen the control activity.

Activity 1	**Controls established for both physical and control system access.**
Activity 2	**Defined access levels established by position.**
Activity 3	**Employee promotions, position changes or termination of employee/contractors initiate a review of access needs.**
Activity 4	**Entity performs periodic reviews of personnel access levels to identified systems to ensure appropriate access is maintained.**
Activity 5	**Changes due to: technology, mergers, acquisitions, infrastructure changes, etc. require a review of all position access.**