MIDWEST RELIABILITY ORGANIZATION

Internal Controls

Frameworks, Concepts, and Positive Examples

Denise Hunter - Director, Corporate Risk Management, Corporate Compliance & Ethics at NERC

Rich Samec - Principal Compliance Engineer at MRO

Content

- Overview of Established Internal Controls Frameworks and Standards
- Highlight Common Terms, Criteria, and Elements
- Positive Examples of Internal Controls

"What can we lean on to establish, communicate, enhance, monitor, and assess our Internal Controls Program?"

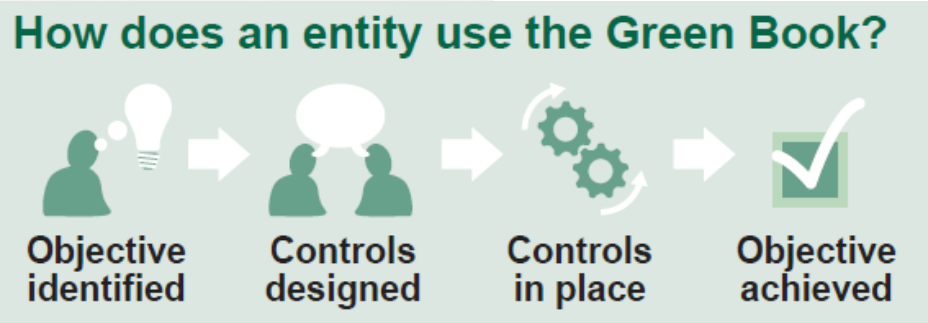
Established Internal Controls Frameworks and Standards

- **COSO**
- **Green Book**
- **Yellow Book (GAGAS)**

COSO
- Framework

Five ***Components*** and seventeen ***Principles***

Green Book
- Standard
- Informs Entities



Yellow Book (GAGAS)
- Standard
- Informs Auditors

Chapter 8 – Performance Assessments

Assess Activities, Sufficient Evidence, and Identify Deficiencies

Common Terms Across Frameworks

Inherent Risk

Control Environment

Control Objectives

Attributes

Design

Component

Control Activities

Competence

Segregation of Duties

Internal Control System

Residual Risk

ERO Approach

Definitions

ERO: Internal controls are the processes, practices, policies or procedures, system applications and technology tools, and skilled human capital an entity employs to address risks associated with the reliable operation of its business.

But Really, an Internal Control Is: Anything you do to ensure that what you want to happen happens, and what you don't want to happen doesn't happen.

Assessments

- Focus on Risk Areas and/or Concerns
- Understand Control Objectives, Design, and Activities
- Walk Through Processes
- Assess the Effectiveness of Controls
- Develop a Conclusion

Some Positive Attributes of an Internal Control

- Risk is Identified, Tied to the Objective
- Activity / Process is Documented and Communicated
- Achievement of Objective Tied to Risk Reduction
- Control Activities are Well Designed
- Control Activities are Implemented and Effective
- Segregation of Duties to Reduce Risks and Increase Effectiveness

Internal Controls System

Maturing to an Entity-Wide Vision

A comprehensive inventory for a medium-sized entity which defines and tracks a detailed vision of the desired end state of a system of Internal Controls.

Entity-Wide Risk Areas

- ***Associated Control Descriptions***
  - ***Whether Implemented***
    - ***Whether Documented***
      - ***Whether Review, Training, Periodicity are Involved***
        - ***Names of Associated Documents***
          - ***Narrative of Issues***

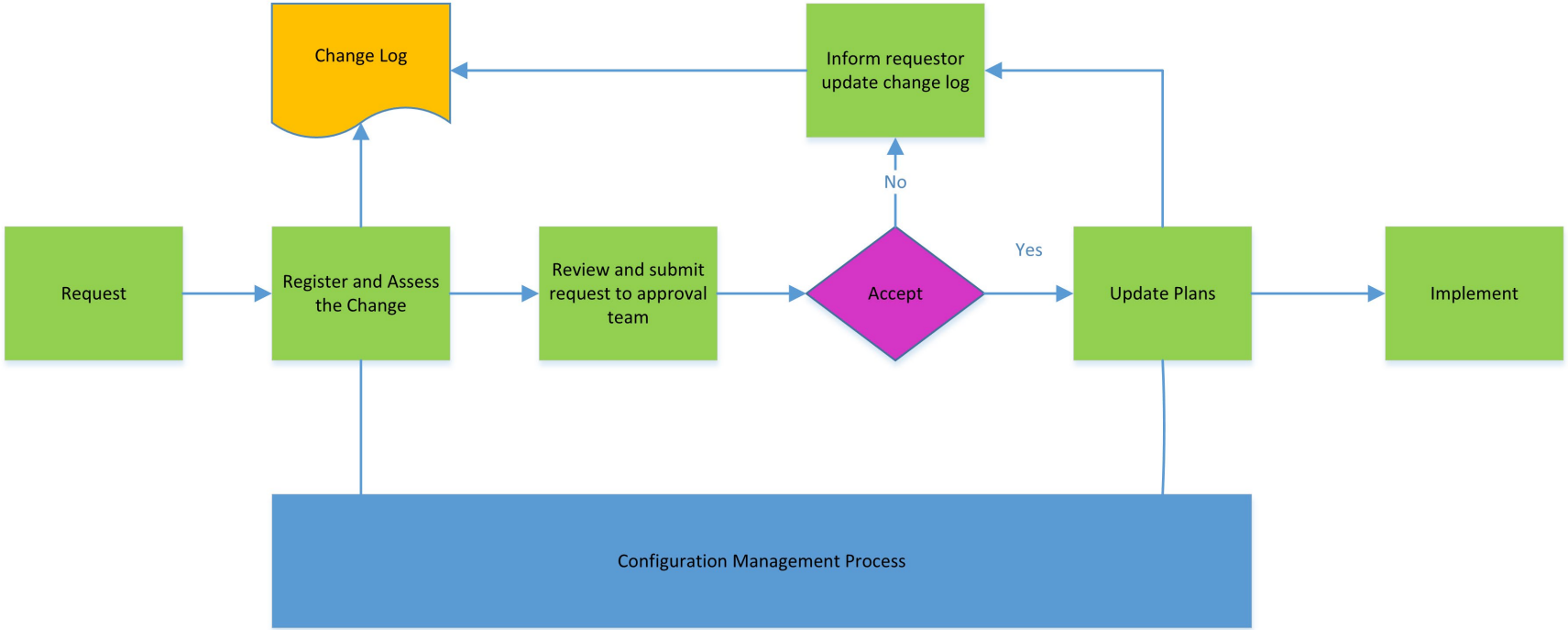
CIP-010-3 Tripwire Application

Implementing a common industry tool which facilitates configuration and change management, and checks integrity

- The entity utilized Tripwire to create a *Configuration Checklist* which is used to set up an asset
- The tool will automatically detect changes to the asset configuration
- The tool is able to revert to the correct baseline configuration if an unintentional change was made

Change Management Controls

Designed to ensure all changes are approved and documented, services aren't unnecessarily disrupted, and resources are used efficiently



Real-time Assessment Controls

Identifying comprehensive criteria for defining your RTA

- Understand your RTA
- “Good” data and sufficient data
- Data from outside source
- Contingencies accepted and rejected
- Root Cause Analysis
- Support studies
- Models managed/maintained
- Analysis expectations
- Overlapping coverage
- Change Management

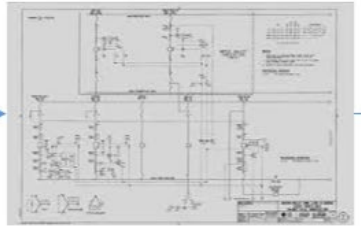
FAC-008-3 Facility Ratings

Controls to facilitate the extent of collection, flow and accuracy of information

Field Elements

- ***"Record Drawings"***
  - ***Facility Ratings Database***
    - ***EMS***
      - ***Planning Models***
        - ***SOL Methodology***

Listing of Substation Equipment



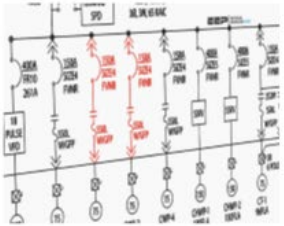
Substation Prints

Facility Ratings Database

Verification Control- methodology to ensure substation listing matches what is in the field

EMS Facility Ratings

Planning Models



Reconciliation: prints and facility ratings database are aligned; facility rating database is aligned with planning models and EMS ratings

Other possible controls:

2nd Party Review
*Clear accountability- who performs the review
*Defined criteria re: what is reviewed
*Defined review process

Contract Mgmt (If applicable)
*Contract meets all Standard/ Req expectations
*Reviewed by knowledgeable person and approved
*Tracked for accuracy and gaps addressed timely

Key Takeaways

- Established frameworks and standards are available and adaptable to our industry
- Common language will improve the flow of controls development and discussion
- Effective controls may utilize sophisticated tools, or not