MIDWEST RELIABILITY ORGANIZATION

Internal Controls Framework

July 28, 2022

Larry Johnson - Principal Compliance Engineer/Auditor (CIP)
Rich Samec - Principal Compliance Engineer/Auditor (O&P)

Larry Johnson

Principal Compliance Engineer/Auditor (CIP)

Larry Johnson joined MRO in July 2018 as a Senior CIP Compliance Auditor. Mr. Johnson transitioned to the role of Principal Compliance Auditor in January 2020.

Prior to joining MRO Mr. Johnson worked for ALLETE/Minnesota Power for over 30 years in Duluth, MN. He has held various IT related positions as a Computer Programmer on their Energy Management System, a Network and Systems Administrator, Information Technology Security Analyst, and Lead Information Systems Auditor. Mr. Johnson has led several compliance initiatives such as; NERC CIP and HIPAA, has taught evening computer and security related courses for Wisconsin Indianhead Technical College, and has presented at several national security conferences such as; CSI, EEI, InfoSec World and IT Security World plus local events on various compliance, security, and SCADA related topics. He maintains CISSP, CISA, and CSSA certifications and is a member of the local IIA, InfraGard, ISACA, ISSA and OWASP Minnesota chapters.

Mr. Johnson is a graduate of the University of Minnesota – Duluth with a Bachelor of Applied Science degree in Industrial Electronics Technology with a minor in Mathematics.

Rich Samec

Principal Compliance Engineer/Auditor (O&P)

Richard Samec rejoined MRO in January 2020 as Principal Compliance Engineer and Auditor in Operations and Planning, after holding the position of Senior Compliance Engineer at MRO from October 2015 through April 2018, where he was an auditor in both CIP and Operations and Planning. Prior to joining MRO, Mr. Samec had a combined 14 years of experience as an Electrical Engineer and Senior Project Manager in the areas of Capacity Planning, Substation Engineering, Metering, SCADA, and CapX2020 Regional Transmission Development. Mr. Samec also had a combined 9 years of experience as an Electrical Engineer and Consulting Engineer, overseeing the design and construction of electrical facilities associated with pipeline facilities, including stations and terminals.

Mr. Samec attended the University of North Dakota, where he earned a Bachelor of Science degree in Electrical Engineering in 1991. Mr. Samec is also a registered professional engineer (PE) in the state of Minnesota.

Recent Outreach

- **July 2021 CMEPAC Conference**
  - ***Internal Controls Frameworks, Concepts, and Positive Examples***

- **April 2022 Webinar**
  - ***MRO CMEPAC Internal Controls Question and Answer Session***

Key Themes Today

- Refresher on Frameworks and Common Language
- Assessing Maturity of an Internal Controls Program
- Examples of Audit Approach
- Q&A

Definition of an Internal Control

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.

"How do you ensure that what you want to happen happens, and what you don't want to happen doesn't happen?"

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

Established Internal Controls Frameworks and Standards

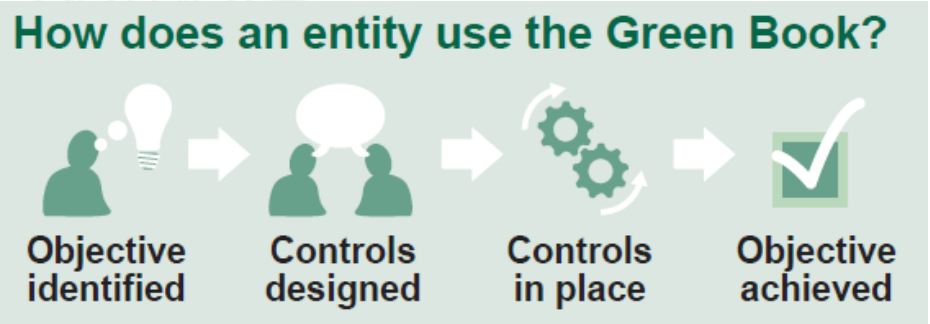
- **COSO**
- **Green Book**
- **Yellow Book (GAGAS)**

COSO
- Framework

Green Book
- Standard
- Informs Entities

Yellow Book (GAGAS)
- Standard
- Informs Auditors

Five *Components* and seventeen *Principles*



Chapter 8 – Performance Assessments

Assess Activities, Sufficient Evidence, and Identify Deficiencies

Common Language

Risk Assessment

Inherent Risk

Failure Points

Control Objectives (Compliance, Operations)

Global Controls

Design

Control Activities

Attributes

Process

Components

Document

Segregation of Duties

Monitoring

Competence

Communication

Implementation

Evaluation

Effective

Internal Control System

Residual Risk

Prior 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

Assessing Maturity

An ERO Internal Controls Task Force is working to develop a Maturity Model

An example of maturity levels within a Maturity Model Framework:

Initial

Developing/Repeatable

Defined

Managed

Optimized

Source: Carnegie Mellon University

Internal Controls System

Maturing to an Entity-Wide Vision

A comprehensive inventory 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***

Audit Approach Examples

"What can I expect during an audit?"

- Notification Packet (ICP Questionnaire) helps inform MRO on an Entity's Compliance Program
- Pre Audit Overview
- Fieldwork Kickoff Presentation
- Entity-wide Internal Controls vs. those specific to Standards and Requirements
- Document Review
  - Inquiry
  - Examination/Inspection of Evidence
  - Observation/Walkthrough

Assessment Approach

"How is an Internal Control Assessed?"

- Risk(s)
- Objective(s)
- Design
- Activities
- Implementation
- Testing and Conclusions

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

Example 1

Global Internal Controls for a Large Organization

Internal Control Assessment

- **Risk(s)**
  - Risk of Non-compliance
- **Objective(s)**
  - Improved Tracking and Reporting
- **Design**
  - Customized Application
- **Activities**
  - Track Reports, Meetings, Include Automation
- **Implementation**
  - Training and Utilization of Application
- **Testing and Conclusions**
  - Observation

Maturity Assessment

- **Initial**
- **Developing/Repeatable**
- **Defined**
- **Managed**
- **Optimized**

Example 2

Global Internal Controls for a Small Organization

Internal Control Assessment

- **Risk(s)**
  - Risk of Non-compliance
- **Objective(s)**
  - Improved Tracking and Reporting
- **Design**
  - Standard Office Application(s)
- **Activities**
  - Track Meetings, Status
- **Implementation**
  - Training and Utilization of Application
- **Testing and Conclusions**
  - Observation

Maturity Assessment

- **Initial**
- **Developing/Repeatable**
- **Defined**
- **Managed**
- **Optimized**

CIP-010-3 R2 – Configuration Monitoring

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

Example 3

CIP – CIP-010-3 R2 – Configuration Management

Internal Control Assessment

- **Risk(s)**
  - Insufficient criteria for monitoring of a baseline
- **Objective(s)**
  - Ensure the criteria for monitoring is functioning properly
- **Design**
  - Criteria is tested, changes update the criteria
- **Activities**
  - Periodically run on test system
- **Implementation**
  - Automated tool like tripwire
- **Testing and Conclusions**
  - Review of evidence, re-performance

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***

Example 4

O&P – FAC-008

Internal Control Assessment

- **Risk(s)**
  - Operating with incorrect facility ratings
- **Objective(s)**
  - Ensure Facility Ratings are correct throughout the system
- **Design**
  - Application to link engineering drawings with EMS database
- **Activities**
  - Verification, Automated Transfer
- **Implementation**
  - Develop and Maintain
- **Testing and Conclusions**
  - Observation

Q&A