MRO Copyright 2007

MIDWEST RELIABILITY ORGANIZATION

COMPLIANCE COMMITTEE

PHASE II

GOVERNANCE RISK PROGRAM

Report Date: January 4, 2013
Updated: April 2018

Authored by

The Midwest Reliability Organization – Performance and Risk Oversight Subcommittee (PROS).

The MRO Subject Matter Expert Team is an industry stakeholder group which includes subject matter experts from MRO member organizations in various technical areas. Any materials, guidance, and views from stakeholder groups are meant to be helpful to industry participants; but should not be considered approved or endorsed by MRO staff or its board of directors unless specified.

Disclaimer

The Midwest Reliability Organization (MRO) Compliance Committee (CC) is committed to providing practical guidance to the stakeholders, by developing tools and processes to assure that both operational and compliance obligations are met including training and non-binding guidance to industry stakeholders regarding existing and emerging Reliability Standards. Any materials, including presentations, were developed through the Compliance Committee by Subject Matter Experts from member organizations within the MRO.

These documents may be reproduced or distributed to any person or entity only in its entirety.

Acknowledgement

This publication was developed by a team of Subject Matter Experts (SME) from MRO member organizations within the MRO footprint. The development of SME teams is an ongoing effort to produce unified application guides for MRO and its Registered Entities.

The PRO's Team Chair, Joe DePoorter from Madison Gas & Electric, wishes to acknowledge and thank those who dedicated efforts and contributed significantly to this publication. The MRO Staff and the MRO Compliance Committee and their organizational affiliations.

TABLE OF CONTENTS

INTRODUCTION

The Midwest Reliability Organization's Performance and Risk Oversight Sub-committee (PROS) made up of selected MRO members, established eight attributes that can be considered to be within a sound *Internal Control Program*. In no way do the PROS intend for these attributes to be used within the ERO's enforceable model, but rather a set of attributes that if implemented (based on entity assigned risk) should enhance Bulk Electric System (BES) reliability by the paradigm shift from detection of non-compliance to prevention of noncompliance. An additional intent of applying the eight attributes to an entity's *Internal Control Program* is to reasonably assure that if noncompliance is detected, the action will not lead to issues that could cause instability, uncontrolled separation, and cascading, per Section 215 of the Federal Powers Act.

The PROS did causative research and has based the sound *Internal Controls Program* (known as the *program*) on the Committee of Sponsoring Organizations of the Treadway Commission (COSO) internal control framework, the Federal Energy Regulatory Commission's 2005 Policy Statement on Enforcement (FERC's 13 Questions), U.S. Department of Justice Evaluation of Corporate Compliance Programs and the MRO's Internal Control Program (ICP) questionnaire. This baseline will assist both the entity and the Compliance Enforcement Authority (CEA) as this is a transparent process where trust is established and the entity's *program* of internal controls will continue to operate effectively, thus supporting the reliability of the BES.

The PROS reviewed the COSO's five components of internal controls; FERC's Policy Statement on Enforcement, U.S. Department of Justice Evaluation of Corporate Compliance Programs, MRO's (ICP) questionnaire and established a baseline to assist Registered Entities in establishing an overall *program* that leverages these current models. Each registered entity should review this document in its entirety and extrapolate the appropriate information, based on risk that the registered entity is willing to accept (called risk appetite or risk tolerance), and enhance its *program*, accordingly.

The PROS believe that each registered entity has an *inherent risk* (its physical make up) associated with each registered function. Each registered entity should also establish *control activities* (the basis of this document and PROS Phase I) to assure that the *inherent risks* are reviewed and mitigated in order to support the reliability of the BES. The PROS recognize that there is "no one size fits all" with regards to an entity's Internal Compliance Program and associated internal controls.

OVERVIEW

The authors of this paper relied on existing frameworks to assist with the development of the Internal Controls Program criteria and have incorporated some of that information into each of the proposed criteria. The 2017 update and review added the U.S. Department of Justice Evaluation of Corporate Compliance Programs. The frameworks include COSO's five interrelated and equally important components: Internal Control – Integrated Framework, MRO ICP Questionnaire, FERC's guidance order of 13 questions, and the U.S. Department of Justice Evaluation of Corporate Compliance Programs. These four existing frameworks are included as Appendix 1, and the PROS would encourage you to evaluate your organization's Internal Compliance Program and associated Internal Controls by measuring them against the frameworks and questions provided in Appendix 1.

<u>Measures:</u>
The PROS established *measures* of success for each attribute to assist Registered Entities in understanding what could be an adequate amount of information for each attribute, always based on the amount of risk that the registered entity is willing to accept. Registered Entities always have the option of increasing, decreasing or customizing *measures* to fit their wants and needs. Measures are not required to be within the registered entity's *program*, but are provided (along with *Test Activities*) as examples the registered entity may use in enhancing its *program*.

<u>Test Activities:</u>
The PROS established *test activities* to assist registered entities in self-governing their *programs*. The established *test activities* are a series of questions that allow the registered entity and the CEA to evaluate the depth and breathe of each attribute. The *test activities* are essentially an "open book test", which provide transparency and can be adjusted to fit the registered entity's *programs*. *Test activities* (and *measures*) are the registered entity's *control activities* that it has incorporated to reduce its *inherent risks*.

<u>Definitions:</u>

<u>Control Activities:</u> The registered entity's programs, processes, and knowledge (maturity) of applying control activities that are established to keep its inherent risks in check. These processes can be living documents that can be enhanced when current programs mature and new inherent risks are discovered or obtained.

<u>Inherent Risk:</u> The registered entity's physical make up that is usually static in nature, e.g.; system size, number of functions, interconnection points, peak load, circuit miles, transmission voltages levels, etc., in essence the registered entity's story.

<u>Operationalized Compliance Program:</u> A compliance program that is known about and used within the registered entity (at all levels) to prevent, detect and correct possible issues with mandatory Standards thus supporting the reliability of the bulk power system.

Reasonable Assurance: The high degree of confidence and certainty based on a given sample size that there is proof that the minimum level of compliance is being met. Note that absolute assurance cannot be obtained due to the amount of resources required by a Compliance Enforcement Agency to prove 100% accuracy.

Residual Risk: The amount of risk remaining after relevant controls has been applied in order to minimize the known risk.

Risk Appetite: The amount of risk that the entity is willing to accept, either before or after controls have been applied to it. Also called Risk Tolerance.

Compliance Model

Audit Structure: CEAs have to know which controls are in place before they ask for evidence of any of those controls. If processes are in place for the registered entity to tests its own controls, the auditors will want to see the results of those processes (tests and measurements) more than they will want to see evidence of each individual test. How much will need to be provided ahead of time? CEAs need reasonable assurance that these activities are taking place. How much of this is within the control of the entity, itself? It is reasonable to focus on the stronger controls that are implemented and collect evidence from those. Can an entity just submit the matrix ahead of the audit and then requests from MRO will be based on those listed items? This will vary as more audits are completed. The evidence burden should be reduced once the CEA understands your *inherent risk* and the design of your *program* that combats your *inherent risks* and provides a level of reasonable assurance.

Attribute 1: Corporate Electric Reliability Compliance Policy / Program

Objective:

A well-documented *Internal Compliance Program* with robust prioritized internal controls is a good business practice that will naturally incent companies to operationalize compliance into their normal business practices, providing management reasonable assurance that reliability and compliance goals are being met. Written policies or procedures will establish the registered entity's commitment to compliance by establishing a baseline for personnel to follow. These governance documents are "soft controls" that set the "tone at the top." These policies or procedures are living documents that, as the entity matures, are enhanced to reflect industry changes and the entity's optimized risk model.

Measures:

Examples may include but are not limited to:

Likely that the entire eight attributes and an associated plan will be described in this document or multiple documents. It should also demonstrate tone at the top and commitment by leadership. Should be easily followed and demonstrate reviews and updates. This can be combined with enterprise programs, if appropriate, based on what's implemented at that particular entity.

Test Activities:

Ask: Is there a documented program? Is it approved and or endorsed by leadership/executives? Is it reviewed and updated as appropriate and periodically? Has there been growth of your program as the industry has grown? Is the program used and followed? If not, change it to meet your current daily processes.

COSO Basis:

- Control Environment
- Control Activities

Regional ICP Survey:

- Questions 1, 9

FERC Question Reference:

- Does the company have an established, formal program for internal compliance?

Criteria:

- Criterion 1 – The registered entity has a written policy / program document(s) that describe the framework and supporting processes used to address the attributes of its Internal Compliance Program. It is best practice to have addressed, in some measure, all eight of the identified attributes. The number of documented policies and program documents will vary from entity to entity. This variance may be due to the size of the entity, scope of the program, and corporate style guides.

- Criterion 2 – The registered entity's policy / program has documented approval by senior management or executive leadership. The approver should, based on his or her position in the organization, have authority to reasonably assure the program is implemented, as well as the ability to allocate resources and personnel to meet/address compliance obligations.

- Criterion 3 – The program document(s) have an established, periodic review cycle to ensure accuracy and alignment with operations. The review and update activities are accessible through document change control processes and/or version history.

Attribute 2: Governance

Objective:
Governance and risk management are interdependent areas of focus within an effective Internal Compliance Program. Entities must identify and manage the many types of risk associated with maintaining the reliability of the BES. An appropriate governance model will allow the entity to respond to and mitigate the identified risks. In addition, a successfully implemented governance program facilitates active leadership oversight in compliance activities and timely reaction to unexpected compliance issues, as they arise, through normal and emergency operations.

COSO Basis:

- Control Environment
- Risk Assessment

Regional ICP Survey:
- Questions 3, 4, 5, 7, 8, 12, 13

FERC Question Reference:
- Is the Internal Compliance Program (ICP) well documented and widely disseminated within the Company?
- Is the Program supervised by an Officer or other high-ranking official?
- Does the Compliance Officer report to or have independent access to the Chief Executive Officer and/or the Board of Directors?
- Is the program operated and managed so as to be independent?
- Are there sufficient resources dedicated to the compliance program?

Measures:
Examples of activities or artifacts upon which measures may be based but are not limited to:
Scheduled/periodic meetings, documentation review/updates, org charts, staffing models, leadership communications, industry participation, committee/board participation/attendance, leadership meeting minutes or summaries, status reports, outreach, customer communications, documented review processes that show independence or cross-departmental assistance, review process that is independent from operations, reporting process, third party contracts (scopes of work, audit reports, summaries, etc.), and third party participation in committees and meetings (potentially independent reporting to leadership).

Test Activities:
Is NERC compliance addressed regularly in leadership meetings? Do you have a process to respond to regulatory inquiries or alerts? Do you have scheduled meetings for oversight groups or committees? Is there a schedule for reporting to leadership or audit committees? Do you have a third party or external review or assessment? Do you have a process to obtain independent review within your organization? Have you reviewed that the measures are in place? Do you allow compliance concerns to be addressed directly with leadership?

Criteria:
- Criterion 1 – <u>Executive involvement:</u> Senior Executives must take an active role in ensuring the compliance activities are implemented in an effective manner across the registered entity. The registered entity's compliance philosophy and direction must start with the executive team, and be reinforced from the top down. There should be routine scheduled status meetings to ensure the Executive team is engaged and involved in the process.

- Criterion 2 – Access to Senior Management (CEO/BOD and/or Council, etc.): The individual charged with responsibility for managing the Compliance Program must have independent access to the Senior Management and policy setting group (BOD, Council, etc.) within the organization. This access must allow for a flow of information in both directions in an accurate and timely manner. It is imperative that Senior Management understand and agree with and actively support the activities being implemented.

- Criterion 3 – Sufficient Staffing (all staff, not just compliance): For a program to be successful it is necessary to ensure there is adequate staff to perform the required activities. There should be a compliance organization (if required by the entity) appropriately staffed, and a sufficient number of technical personnel and Subject Matter Experts (SME's), trained to understand what is required including the internal controls for the organization.

- Criterion 4 – Independent Compliance Staffing: Personnel assigned to assessing compliance should report through a leadership structure that allows independence from the operating areas fo which the compliance activities are implemented. Independence can be achieved through a permanent, organizationally-isolated compliance area, third party resources, or any resource allocation that, within the organization, separates the evaluation function from the operational function for the specific activity.

- Criterion 5 – Effectively Assess & Prioritize Risk: Complete compliance and operational risk inventories allow the entity's leadership to assess and prioritize the identified NERC/enterprise/organization-level risks such that resources can be allocated to monitor, mitigate, and respond to events with potentially negative impact on the entity, or reliability of the BES. Criteria for assessing and prioritizing the risks need to be well-documented, as well as consistently and regularly applied. Additionally, the process for identifying, assessing, and prioritizing risk must be reviewed and updated periodically based on changes in industry, regulatory, or operational information.

- Criterion 6 – Effective Leadership Engagement and Oversight: The governance model should include a formal framework for internal and external communication in order to reasonably assure that leadership, impacted personnel, regulators, and stakeholders have current knowledge of implementation status, operational or compliance issues, and performance metrics. Transparency, within the constraints of the entity's information protection program, permits leadership visibility into and situational awareness of the compliance program and allows appropriate regulator engagement, when necessary.

- Criterion 7 – Adaptability: The entity should have a documented and implemented change management program which allows flexibility and includes provisions for document, program, and regulatory changes. The entity should be able to identify the need for, track, and document modifications throughout the change lifecycle. Change control rigor will include appropriate review and approval cycles, as well as dissemination to impacted personnel and leadership.

Attribute 3: Internal Control Framework (ICF) – Internal Controls and Risk Prioritization

Objective:
An internal control is a process designed to provide reasonable assurance regarding the achievement of objectives. The internal control framework should cover all aspects of risks, controls, and activities and allow the entity to effectively meet its objectives (i.e., to operate the BES in a safe and reliable manner). Preventive and detective controls should correlate to, monitor, manage, and mitigate identified and prioritized risks.

Measures:
Risk inventories, documented risk identification processes, roles and responsibilities for prioritizing risks, roles and responsibilities for control ownership, implemented detective controls, implemented preventive controls.

Test Activities:
Did you assign controls to the risks? Do controls have owners? Are controls reviewed/monitored/tested based on risk? Are the controls performed and working properly? What is the output of the controls? Do the controls monitor the key variables? Do the controls meet the objectives? Do you have a process for identifying and updating risks? Do you have a process for modifying controls?

COSO Basis:

- Control Activities

Regional ICP Survey:
- Questions 11, 12, 13, 14?

FERC Question Reference:
- Important questions to identify and prioritize risk:
- Have you identified the risks?
- Have you identified key risks?
- Have you prioritized key risk?
- Have you identified internal controls appropriate to the risks?
- Have you identified performance metrics for key risks?

Criteria:

- Criterion 1 – Identify and Prioritize Risks: The entity should have a method for identifying the reliability risks facing the organization. Additionally, the entity should have criteria or methods for ranking or assessing risk such that risks can be prioritized and resources can be effectively allocated to manage the highest risks.

- Criterion 2 – Assign and Perform Controls: The entity should have a method to identify controls and assign those controls to an accountable party in order to manage and mitigate the prioritized risks. The entity should be able to demonstrate that the controls are working properly and meeting the assigned objective.

- Criterion 3 – Monitor and Modify Controls: The entity should periodically evaluate the performance of the controls to assure effective implementation and execution. The entity should have processes to modify controls, as necessary, based on performance reviews, regulatory changes, process improvement, etc.

Attribute 4: Independent Review

Objective:
An excellent practice for any internal compliance program is the process of periodic independent review of the program. An effective program is one that focuses on the right objectives (eight attributes identified in this guidance), functions effectively, and provides the desired results (reliability and compliance goals are being met). An independent review of the program will help an entity get there. Items that should be considered in the process of an independent review include management support, type of review, reviewer qualifications, review objectives, and issue follow-up.

Measures:
Examples may include but are not limited to:
Updates were made from recommendations of an independent review. The (independent) review has confirmed the entity's objectives are being met. The review confirmed that resources are being applied to the highest entity assigned risk areas.

COSO Basis:

- Monitoring
- Control Environment

Regional ICP Survey:

- Questions 5, 6, 9, 14?

FERC Question Reference:

- Is the program operated and managed so as to be independent?
- How frequently does the company review and modify the compliance program?

Test Activities:
Has there been an independent review of your program? Were outcomes (recommendations) of the independent review accepted by the entity? Has the program been enhanced as required by the entity? Is there a systematic review process of the program?

Criteria:

- Criterion 1 – <u>Management Support:</u> Management support of the independent review process is essential. As part of an entity's control environment, management support sets the tone for the organization, letting its people know that this is important, as is the overall success of the internal compliance program. Management support should be evidenced by management's involvement in choosing/approving the review group and type of review, making available sufficient personnel to participate in the review, participating in relevant meetings, and following-up on results.

- Criterion 2 – <u>Type of Review:</u> The independent review can be performed by either an internal corporate group outside of the compliance program (i.e., internal audit) or by an external third party. If the review is by an external third party, an excellent option is a peer review. A peer review is a process of self-regulation or review by a profession/industry or a process of evaluation involving qualified individuals within the relevant field. Peer review methods are employed to help maintain standards, improve performance and provide credibility. The advantage of the peer review is that it involves individuals from the specific industry (electric utility) who are experienced in the field and can provide great input. As an example, The Transmission Owners/Operators Forum provides the opportunity for entities to participate in a peer review program.

- Criterion 3 – Reviewer Qualifications: There are many organizations that will provide independent review of an entity's program. When choosing a review group the entity must be sure the individuals involved have sufficient experience in the industry or in the Compliance or Audit fields. The following should be considered:
    - How many reviews has the group performed?
    - How much experience does the group have in the industry?
    - How much experience does the group have in the Compliance or Audit field?
    - Ask the group for a list of entities for which it has conducted peer reviews.
    - Are there any other value-added services that the group can provide during the peer review?

- Criterion 4 – Review Objectives: The objective of the independent review is to provide feedback and suggestions on the overall performance of the internal compliance program. As such, the independent review should try to cover all aspects of an entity's internal compliance program. As an example, all of the attributes identified in this guidance should be included in the review: Compliance Policy/Program; Governance; Internal Control Framework; Regulatory Integrity; Corrective Action Program; Training and Awareness; and Continuous Improvement. The entity should determine the review frequency of the internal compliance program and who in the entity should initiate the review.

    - Prior to the review the entity should be in contact (i.e., documented meetings, phone calls, emails) with the review group to determine the specifics of the review. It should also be determined what should be made available prior to the review and then during the on-site review. During the review, the entity must be open and honest with the review team to gain benefit from the review. You must also have sufficient team members to work with the review group. The end result of the review should include a report identifying the results and any suggested improvements. The report should be shared with all relevant parties within the entity.

- Criterion 5 – Issue Follow-up: All identified issues, deviations, and suggestions identified during the review should be subject to follow-up actions. All items identified should be discussed with the reviewers to be sure there is a clear understanding of the suggestion. Each item should be evaluated and a determination made as to whether further activity will be pursued on the item. All items deemed for further action should be maintained within a tracking log. The tracking log should be regularly reviewed for progress until completion.

Attribute 5: Regulatory Integrity

Objective:
Effective communications and interactions with the Regional Entities and NERC are important attributes of an Internal Compliance Program. Communications and interactions with NERC and Regional Entity compliance and enforcement staffs should be done with transparency and

integrity. Registered entities should administer programs which assure responsiveness and conformance to the compliance monitoring discovery methods and enforcement protocols defined in the Compliance Monitoring and Enforcement Program. Registered entities must assure all commitments made to the regulators are timely fulfilled. The overall objective of this attribute is to assure that the registered entity communicates and interfaces confidentially, timely, and credibly with the Regional Entities and NERC.

Measures:
Examples may include but are not limited to:
Responsiveness to MRO data requests, timely submittals, complete analysis, thorough documentation that meets MRO expectations/objectives, candid and conversational tone in MRO interactions, good relationship/rapport, culture of cooperation. Registered entity's involvement with current industry topics and trends whereby requested input (data) has been received in a timely manner.

COSO Basis:

- Control Environment
- Information & Communications

Regional ICP Survey:

- Questions 12, 13

Test Activities:
Do you have an adversarial relationship with the regulators? Do you have a good working rapport with the regulator? Do you meet the deadlines for your submissions and compensating measures? Are your submissions complete, accurate, and transparent? Do your submissions require frequent or numerous follow-up interactions due to missing, confusing, or questionable information? Has your entity been asked to assist a regulator in the development, implementation or review of current trends or topics?

Criteria:

- Criterion 1 – <u>CMEP Obligations are Effectively Satisfied:</u> The NERC Compliance Monitoring and Enforcement Program (CMEP) defines a variety of compliance monitoring discovery methods. Registered entities are expected to administer programs and processes to assure that the CMEP obligations are satisfied and associated regulatory filings are of high quality and timely made.

- Criterion 2 – <u>Fulfillment of Commitments</u>: While administering the compliance monitoring discovery methods defined in the Compliance Monitoring and Enforcement Program a registered entity will likely need to make commitments to the Regional Entities and/or NERC. The commitments may come in the form of mitigation plan action items, TFE compensating measures, settlement agreement actions, event analysis recommendations, and NERC Alert actions items, etc. Registered entities must assure that these commitments are fulfilled in a timely manner.

- Criterion 3 – <u>Communicate with Transparency and Integrity</u>: Registered entities are expected to maintain credibility with the Regional Entities and NERC. Credibility is built by effectively administering programs which meet the CMEP obligations and enforcement processes and is reinforced by communicating with transparency and integrity with the regulators.

Attribute 6: Corrective Action Program

Objective:
An enterprise/organization-level Corrective Action Program (CAP) is a key component of an effective internal controls process. This process encompasses:

- monitoring of performance to identify problem findings (or near misses),
- determining the causes of performance problems,
- implementing corrective actions to resolve the problems and to minimize the probability and severity of a recurrence, and
- determining the effectiveness of the corrective actions to ensure successful resolution and prevention of the same or similar problems.

Measures:
Examples may include but are not limited to:
Documented program with defined thresholds, approved program, cause/effect or root cause analysis documentation or process, mitigations or action plans, analysis of recurrence, trending analysis for deficiencies, responses, evaluation of impact on risk, human performance indicators or measurements, near-hit analysis.

Test Activities:
Do you have a documented CAP? Are your thresholds defined and consistently implemented? Do you identify corrective action plans? Do you have a process to recognize trends or human performance issues? Have you reduced reoccurrence of issues? Do you have a process/structure for conducting a cause/effect or root cause analysis? Do you know the status of your corrective action plans?

COSO Basis:

- Monitoring
- Control Activities

Regional ICP Survey:

- Questions 12, 13

FERC Question Reference:

- How has the company responded to prior wrongdoings?
- Does the company adopt and ensure enforcement of new and more effective internal

Criteria:

- Criterion 1 – Approved program document: Documented and approved program documents (could include templates for different CAPs) can ensure consistency of application and quality of evaluations and corrective actions.

- Criterion 2 – Defined threshold to enter the corrective action program: The program document should define a threshold for entering the program. The program should be entered for all events related to reliability of the Bulk Electric System (BES) and "near hits" that don't cause events, but should be addressed based on risk of a similar issue causing an event in the future.

- Criterion 3 – Assess or investigate events based on their significance: The level of assessment or evaluation of issues should be based on the risk associated with lack of correction of the issue. Low risk issues may be evaluated by a single person only addressing the direct cause while those of high risk may garner an evaluation team with a full root cause and actions to prevent occurrence. It is important for management to allow the process to work and determine the cause and not jump directly to corrective actions.

- Criterion 4 – <u>Develop corrective actions based on cause to reduce the probability of recurrence:</u> Corrective actions should be focused on the cause(s) of the issue as determined by the evaluation. If the causal factors are removed or mitigated, the probability of recurrence of the issue will be significantly reduced. The corrective actions must be directly linked to the cause(s).

- Criterion 5 – <u>Track and trend past similar events:</u> It is important to know how often certain issues are recurring. A low risk event that is rare may need no more than correction of each event as it occurs. However if it happens often, the overall risk of the event is higher, and the significance of the response should be commensurate with that. Trending can likewise indicate when actions taken to correct higher risk issues have been ineffective.

Attribute 7: Training and Awareness

Objective:
Effective training and communication initiatives support a robust compliance program by ensuring that executive and business area management are setting expectations for compliance, and that responsible personnel are appropriately identified and understand their compliance obligations. Layered training that is sufficient (based on the entity's priorities), scoped and in-depth ensures awareness of the regulations and of the criticality of complying with those regulations, and ensures that responsible personnel know how to perform their operational tasks safely and reliably while remaining in compliance. The training at all levels within the entity will promote established compliance activities thus assuring the operationalization of the compliance program.

Measures:
Examples may include but are not limited to:
Training content, training records for completion, comprehension quizzes, posters, brochures, emails, newsletters, websites, evidence of receipt, meeting minutes, and/or orientation packages.

Test Activities:
Do you have a documented training program? Do you have an inventory of required or recommended attendees? Can you demonstrate that required attendees have completed training? Do you have a process for identifying new employees or job changes that require training? Is the content of training relevant to the objectives and are they current?

COSO Basis:
- Information and Communication

Regional ICP Survey:
- Questions 2, 10

FERC Question Reference:
- Is the ICP well-documented and widely disseminated within the company?
- How frequently is training provided to all relevant employees?
- Is the training sufficiently detailed and thorough to instill an understanding of relevant rules and the importance of compliance?

Criteria:

- Criterion 1 – Dissemination of Compliance Program: Training and awareness programs should include the dissemination and communication of Internal Compliance Program policies and procedures to all employees and contractors with direct responsibility for or oversight of implementation (i.e., identification of the appropriate individuals to be responsible for compliance, and awareness of those responsibilities). In addition, entities should assure the availability of compliance program information to all employees and contractors (i.e., identification of compliance contacts, information and program documents widely available within company).

- Criterion 2 – Access to Senior Management (CEO/BOD and/or Council, etc.): The individual charged with responsibility for managing the Compliance Program must have independent access to the Senior Management and policy setting group (BOD, Council, etc.) within the organization. This access must allow for a flow of information in both directions in an accurate and timely manner. It is imperative that Senior Management understand and agree with the activities being implemented.

- Criterion 3 – Awareness Communications:
  - Does the registered entity's internal compliance program require compliance training for its staff, for contractors who have direct responsibilities or for those who may direct the implementation of the processes and procedures that demonstrate compliance with the NERC Reliability Standards? Does the registered entity provide compliance training to its management staff, system operators, engineers, technicians, safety and security staff, vegetation management staff, or other subject matter experts?
  - How does the registered entity keep its management staff, system operators, engineers, technicians, safety and security staff, vegetation management staff, or other subject matter experts current with revisions to the NERC Reliability Standards?
  - Does the registered entity's internal compliance program incorporate methods for providing its management staff, system operators, engineers, technicians, safety and security staff, vegetation management staff, or other subject matter expert's awareness of new compliance interpretations, practices, or procedures?
  - How has the registered entity implemented the plans, policies, and procedures within its internal compliance program? Does the registered entity retain logs, meeting minutes, forms, agendas, or other records to provide reasonable assurance that the internal compliance program is being implemented as intended?

Attribute 8: Continuous Improvement

Objective:
An Internal Compliance Program should include a mechanism for continuous program improvement to provide assurance that internal controls are effective, working properly, and improve reliability. An Internal Compliance Program should be constantly adapting by utilizing information obtained from the program, assessing that information and by evaluating any changes to the program to assure effectiveness. Continuous improvement within an internal compliance program opens communication channels, builds trust, encourages accountability, and identifies opportunities for innovation.

Measures:
Examples may include but are not limited to:
Demonstrating industry participation, documented processes for obtaining and evaluating available information, documented programs for incentive and disciplinary action related to performance, change with merging threats and risks.

Test Activities:
Do you have documented evidence of the review of information or participation in committees, etc.? Has your internal compliance program been updated to implement newly acquired enhancements?

Criteria:

- Criterion 1 – <u>Regulatory and Industry Awareness:</u> Entities are encouraged to take advantage of available, educational resources and participate in compliance outreach activities conducted by entities such as, but not limited to; NERC, Regional Entities, Trade Organizations, Compliance Forums and Groups, Compliance Consultants, or other registered entities?

  Entities are encouraged to maintain ongoing awareness of the regulatory environment, including, proposed or revised Reliability Standards, Implementation Evidence, NERC Data Requests, NERC Alerts, and other compliance documentation subject to industry review.

- Criterion 2 – <u>Internal Performance</u>: The entity should incorporate lessons learned from internal processes, self-assessments, audits, and reviews into the Internal Compliance Program. The entity should encourage personnel to research and implement improved practices. The entity should create a culture that is receptive to employee recommendations for process improvement and implement mechanisms to support the program.

COSO Basis:

- Monitoring

Regional ICP Survey:
- Questions 9, 10, 14

FERC Question Reference:
- How frequently does the company review and modify the compliance program?
- How has the company responded to prior wrongdoings?
- Does the company adopt and ensure enforcement of new and more effective internal controls and procedures to prevent a recurrence of misconduct?

- Criterion 3 – Performance Management: The entity's internal compliance program should provide for compensation, awards, employee recognition, or other incentives (monetary or non-monetary) to encourage compliance with the NERC Reliability Standards?

  The registered entity should incorporate accountability for compliance into relevant employee performance standards for senior management, mid-level management staff, system operators, engineers, technicians, safety and security staff, vegetation management staff, or other subject matter experts.

  The entity's internal compliance program should be supported by a documented code of conduct that may include provisions for disciplinary action for employees involved in willful violation or misconduct relating to the compliance requirements.

Summary

The Performance and Risk Oversight Sub-committee (PROS) has been charged by MRO's Compliance Committee with designing and developing practical guidance that can be utilized by stakeholders to promote transparency and a "Do It yourself" culture of compliance accountability. The eight attributes written within this *Governance Risk Program* are not mandatory but rather represent what *success should look like* in an entity's compliance program. The entity may expand or contract these eight basic attributes depending on the identified risks that are associated with the entity's current compliance program, thus supporting the reliability of the BES.

The PROS started with the higher priority of designing clear controls (Phase I) that would allow an entity to self-govern its compliance program with emphasis on prevention rather than detection of non-compliance. The eight attributes of Phase II take a step back and provide guidance on the entity's overall compliance program. The guidance contained in Phase I is an expansion of the third attribute, Internal Control Framework.

The PROS believe that a self-governing model allows for transparency with our regulators, establishes a good working rapport by eliminating the "us and them" mentality, and supports a stronger culture of compliance with the ultimate end state of a more reliable BES.

About the Authors

All of the authors have been involved with the NERC compliance efforts at their organizations. During that time, they have all gathered compliance experience and knowledge through the design and maintenance of Compliance programs, collaboration with industry peers, mock and documentation audits with internal and third-party audit groups, and sufficiency audits and spot-checks.

The PROS members are all volunteers and believe that the industry can provide the best expertise in developing self-governing models whereby the reliability of the BES can be maintained and enhanced based on future identified risks.

The PROS would like to thank each member and guest that contributed to this project and thank MRO for allowing us to develop and share this document.

Appendix 1

COSO's five interrelated and equally important components: Internal Control – Integrated Framework:

Design and operation of the system of internal controls

1. *Control environment:*

   The control environment sets the tone of an organization by influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include: the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the way in which management assigns authority and responsibility and in which it organizes and develops people; and the attention and direction provided by the board of directors (upper management)

2. *Risk assessment:*

   Every entity faces and must assess a variety of risk from external and internal sources. A precondition for risk assessment is establishing objectives at appropriate levels in the organization. Risk assessment is the identification and analysis of risk relevant to realizing objectives, and it serves as a basis for determining how risks should be managed. Because economic, industry, regulatory and operating conditions will continue to change, flexible mechanisms are needed to identify and address the special risk associated with change.

3. *Control activities:*

   Control activities are the policies and procedures that help assure that management directives are carried out and that necessary actions are taken to address risks to achieving objectives. Control activities are implemented throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews, of operating performance, security of assets and segregation of duties.

4. *Information and communication:*

   Pertinent information is identified, captured, used at all levels of the company, and distributed in a form and timeframe that achieves the objective. Acquired information can be communicated to internal and external audiences.

5. *Monitoring:*

   Monitoring processes are designed and implemented to provide information on whether the internal control system operates effectively over time and internal control deficiencies are identified and communicated in a timely manner to those parties responsible for taking action and to manage as appropriate.

MRO ICP Questionnaire:

The eight attributes, collectively, should address the questions for each region's ICP survey. The MRO's survey is as follows:

1. Does your organization have a formalized (i.e. written) internal compliance program with regard to Reliability Standards? If yes, please explain the scope of the internal compliance program which addresses the NERC Reliability Standards.
2. Please state the extent to which the internal compliance program is distributed within your organization (please include information on training, workshops, newsletters, mailings, and other relevant information which demonstrate effective communications and/or measurements of compliance). For example, does you internal compliance program include a "whistle blowing" procedure?
3. Please identify the person(s) and title(s) of who is responsible for compliance with Reliability Standards (e.g. Compliance Manager, Corporate Compliance Officer or other position).
4. Please provide an organization chart which includes supervision levels (i.e. "chain of command") and responsibilities, and provide a detailed explanation of the supervision and decision-making structure related to internal compliance program.
5. Please explain the relative independence of the compliance responsibilities within the organization from operations. For example, do those with compliance responsibilities have direct access to senior-level executives (e.g. including the Chief Executive Officer, President) and/or Board of Directors? Please provide sufficient details in your response.
6. Please state whether the internal compliance program is operated and managed in a manner that is independent from departments responsible for performance to the Reliability Standards. Please explain your response.
7. Please state the resources (in terms of full time equivalents, positions, or budgets), dedicated to the internal compliance program. Are there unfilled positions related to the internal compliance program or, in your opinion, are there sufficient resources dedicated to the internal compliance program? Please explain.
8. Please explain senior management's role in the internal compliance program. Is there active, regular participation? Is there senior executive sponsorship of the internal compliance program? Please explain.
9. Please explain the review frequency of your internal compliance program. Who initiates the review of the internal compliance program? Please explain.
10. How does your internal compliance program ensure that employees understand the appropriate Reliability Standards that apply to their jobs? Please explain.
11. Please explain the frequency of self-audits and self-assessments within your internal compliance program. Who performs self-audits and self-assessments related to the internal compliance program?

12. Please provide details on corrective action plans when a potential violation of a Reliability Standard(s) is discovered, including disciplinary procedures for applicable employees.
13. Please explain the controls in place to prevent the re-occurrence of the violation in your internal compliance program.
14. Please provide any additional information which may demonstrate the effectiveness of your internal compliance program which was not addressed in this questionnaire.

FERC's guidance order of 13 questions:

1. Does the company have an established, formal program for internal compliance?
2. Is the ICP well documented and widely disseminated within the company?
3. Is the program supervised by an officer or other high ranking official?
4. Does the compliance official report to or have independent access to the CEO or the BOD?
5. Is the program operated and managed so as to be independent?
6. Are there sufficient resources dedicated to the compliance program?
7. Is the compliance fully supported by senior management? For example, is senior management actively involved in compliance efforts and do company policies regarding compensation, promotion, and disciplinary action take into account the relevant employee's compliance with reliability Standards and the reporting of violations?
8. How frequently does the company review and modify the compliance program?
9. How frequently is training provided to all relevant employees?
10. Is the training sufficiently detailed and thorough to instill an understanding of relevant rules and the importance of compliance?
11. In addition to training, does the company have an ongoing process for auditing compliance with reliability Standards?
12. How has the company responded to prior wrongdoings? Did it take disciplinary action against employees involved in violations? When misconduct occurs, is it a repeat of the same offense or misconduct of a different nature?
13. Does the company adopt and ensure enforcement of new and more effective internal controls and procedures to prevent a recurrence of misconduct?

U.S. Department of Justice Evaluation of Corporate Compliance Programs:

The U.S. Department of Justice Evaluation of Corporate Compliance Programs recognizes that each company's risk profile and solutions to reduce its risks warrant particular review to assure the effectiveness of their corporate compliance program. The Evaluation questions have been slightly changed from direct questions concerning after the fact (detective) investigation of noncompliance (fraud) issues to what questions should the entity ask themselves about their ICP, thus focusing on preventive and predictive controls. Along with *Attribute 8: Continuous Improvement*, this evaluation asks common questions that you may wish to ask yourself to assist in reviewing your ICP to reasonably assure that it remains effective. These questions (in whole or part) can be used by the Entity to assist in establishing or enhancing a compliance program as its risks evolve. The PROS has elected to keep these nine sections separate from the eight identified *Attributes* of the Internal Compliance Program for self-auditing and self-evaluation purposes.

1. Analysis and Remediation

Root Cause Analysis – Does the ICP have a root cause analysis process to investigate noncompliance when discovered? Are systemic issues identified as an output of the root cause analysis? Are nonaffiliated people in the company, involved in making the analysis and determining its outcome when noncompliance is discovered?

Prior Indications – Are there controls to discover (prior opportunities) or detect the possible noncompliance in question, such as audit reports identifying relevant control failures or allegations, complaints, or investigations involving similar issues? Is there an ICP analysis of why such opportunities were missed, if any?

Remediation – Does the Entity have specific recommendations to reduce the risk that the same or similar issues will not occur in the future, when noncompliance is discovered within the ICP?

2. Senior and Middle Management

Conduct at the Top – How are senior leaders informed of noncompliance when discovered? Have concrete actions been taken to demonstrate leadership in the company's compliance and remediation efforts when noncompliance is discovered? How does the company monitor its senior leadership's behavior? How has senior leadership modeled proper behavior to subordinates?

Shared Commitment – What specific actions have senior leaders and other stakeholders (*e.g.*, business and operational managers, Finance, Procurement, Legal, Human Resources) taken to demonstrate their commitment to compliance, including their remediation efforts of discovered noncompliance? How is information shared among different components (departments) of the company?

Oversight – What compliance expertise has been available on the board of directors/senior leadership? Have the board of directors/senior leadership and/or external auditors held executive or private sessions with the compliance and control functions? What types of information have the board of directors and senior management examined in their exercise of oversight in the area in which the noncompliance occurred?

3. Autonomy and Resources

Compliance Role – Are compliance personnel involved in training and decisions relevant to a prevention and possible discovered noncompliance issue? Did the compliance or relevant control functions (*e.g.*, Legal, Finance, or Audit) ever raise a concern in the area where the noncompliance occurred prior to discovery?

Stature – How has the compliance function compared with other strategic functions in the company in terms of stature, compensation levels, rank/title, reporting line, resources, and access to key decision-makers? What has been the turnover rate for compliance and relevant control function personnel? What role has compliance personnel played in the company's strategic and operational decisions? Has it been effective in assuring a culture of compliance is maintained within the company?

Experience and Qualifications – Have the compliance personnel had the appropriate experience and qualifications for their roles and responsibilities? Are compliance personnel involved in Regional and NERC level compliance processes?

Autonomy – Do the compliance and relevant control functions had direct reporting lines to anyone on the board of directors, senior leadership? How often do they meet with the board of directors/senior leadership? Are members of the senior management present for these meetings? Who reviews the performance of the compliance function and what is the review process? Who has determined compensation/bonuses/raises/hiring/termination of compliance personnel? Do the compliance and relevant control personnel in the field have reporting lines to headquarters? If not, how has the company ensured their independence?

Empowerment – Have there been specific past instances where compliance raised concerns or objections in the area in which the noncompliance occurred? How has the company responded to such compliance concerns? Have there been specific "close calls" more closely examined as a result of compliance concerns?

Funding and Resources – How have decisions been made about the allocation of personnel and resources for the compliance and relevant control functions in light of the company's risk profile? Have there been times when requests for resources by the compliance and relevant control functions have been denied? If so, how have those decisions been made and why?

4. Policies and Procedures

a. Design and Accessibility

Designing Compliance Policies and Procedures – What is the company's process for designing and implementing new policies and procedures? Who has been involved in the design of policies and procedures? Have business units/divisions been consulted prior to rolling them out? Are they frequently updated?

Applicable Policies and Procedures – Does the company have policies and procedures that prohibited noncompliance actions? How has the company assessed whether these policies and procedures have been effectively implemented? How have the functions that had ownership of these policies and procedures been held accountable for supervisory oversight?

Accessibility – How has the company communicated the policies and procedures relevant to its compliance program to relevant employees and third parties? How has the company evaluated the usefulness of these policies and procedures?

b. **Operational Integration**

Responsibility for Integration – Who has been responsible for integrating policies and procedures within the company's compliance program? With whom have they consulted (*e.g.*, officers, business segments)? How are they been rolled out (*e.g.*, do compliance personnel assess whether employees understand the policies)?

Controls – Are controls in place to detect or prevent noncompliance actions? Are these controls adequate based on the company's risk profile? How are the controls validated to the company's risk profile? What steps have been taken to remedy any failures identified in the control processes?

5. Risk Management Process – What methodology does the company use to identify, analyze, and address possible risks of noncompliance?

Information Gathering and Analysis – What information or metrics has the company collected and used to help detect a possible noncompliance issue? How has the information or metrics informed the company's compliance program?

6. Training and Communications

Risk-Based Training – What training has employees in relevant control functions received? Has the company provided tailored training for high-risk and control employees that addressed the risks within an Inherent Risk Assessment? What analysis has the company undertaken to determine who should be trained and on what subjects?

Form/Content/Effectiveness of Training – Has the training been offered in the form and language appropriate for the intended audience? How does the company measured the effectiveness of the training?

Communications about Noncompliance – What has senior management done to let employees know the company's position on the misconduct concerning noncompliance issues? What communications have there been generated when an employee is disciplined/terminated for failure to comply with the company's policies, procedures, and controls (*e.g.*, anonymized descriptions of the type of noncompliance that leads to discipline)?

Availability of Guidance – What resources have been available to employees to provide guidance relating to compliance policies? How has the company assessed whether its employees know when to seek advice and whether they would be willing to do so?

7. Confidential Reporting and Investigation

Effectiveness of the Reporting Mechanism – How has the company collected, analyzed, and used information from its internal (audit, ethics point, etc.) reporting mechanisms to update its compliance program? How would (does) the company assess the seriousness of the allegations of noncompliance? Has the compliance function had full access to reporting and investigative information?

Properly Scoped Investigation by Qualified Personnel – How has the company ensured that the investigations have been properly scoped, and were independent, objective, appropriately conducted, and properly documented?

Response to Investigations – Has the company's investigation been used to identify root causes, system vulnerabilities, and accountability lapses, including among supervisory manager and senior executives? What is the process for responding to investigative findings? How high up in the company do investigative findings go?

8. Incentives and Disciplinary Measures

Accountability – What disciplinary actions does the company take in response to the noncompliance when it occurs? Are managers (subject matter experts) held accountable for the noncompliance that occurred under their supervision? Does the company's response consider disciplinary actions for supervisors' failure in oversight? What is the company's record (*e.g.*, number and types of disciplinary actions) on employee discipline relating to a substantiated noncompliance issue? Has the company ever terminated or otherwise disciplined anyone (reduced or eliminated bonuses, issued a warning letter, etc.) for a noncompliance issue?

Human Resources Process – Who participated in making disciplinary decisions for a noncompliance issue?

Consistent Application – Are disciplinary actions and incentives been fairly and consistently applied across the organization?

Incentive System – How has the company incentivized compliance and ethical behavior? How has the company considered the potential negative compliance implications of its incentives and rewards? Have there been specific examples of actions taken (*e.g.*, promotions or awards denied) as a result of compliance and ethics considerations?

9. Continuous Improvement, Periodic Testing and Review

Internal Audit – What types of audits are used to identify issues relevant to possible noncompliance? How often do audits occur and how are findings published? What types of relevant audit findings and remediation progress have been reported to management and the board on a regular basis? How have management and the board followed up? How often has internal audit generally conducted assessments in high-risk areas?

Control Testing – Has the company reviewed and audited its compliance program in the area relating to the misconduct, including testing of relevant controls, collection and analysis of compliance data, and interviews of employees and third-parties? How are the results reported and action items tracked? What control testing has the company generally undertaken?

Evolving Updates – How often has the company updated its risk assessments and reviewed its compliance policies, procedures, and practices? What steps has the company taken to determine whether policies/procedures/practices make sense for particular business segments/subsidiaries?