

FERC Reliability Technical Conference

Panel III: ERO Initiatives

Remarks of Jerry A. Hedrick, Jr. - CFE

Director of Regional Entity Assurance and Oversight

North American Electric Reliability Corporation

June 10, 2014

Introduction

Acting Chairman LaFleur, Commissioners, staff, and fellow panelists. My name is Jerry Hedrick and I am the Director of Regional Entity Assurance and Oversight at NERC. I want to thank the Commission for holding this conference today and for providing an opportunity to discuss compliance activities related to the Reliability Assurance Initiative. Today I will provide an update on the RAI compliance pilot program status, lessons learned, framework design elements relative to control evaluation, and implementation considerations.

RAI Pilot Project Status

Since the adoption of RAI by the ERO in early 2013, selected Regional Entities began adapting generally accepted professional audit and internal control guidance¹ to support the implementation of a risk-based approach to compliance monitoring. Partnering with industry, the ERO executed a series of pilots and developed evaluation criteria to assess the pilot design. Since the completion of the pilots in February of 2014, the ERO, again working with selected industry representatives, reviewed the pilot programs and developed a common agreed upon RAI Oversight Plan Framework (Framework) that will serve as structure for the final design. The Framework establishes the key elements for the assessment of risk, evaluation of controls, determination of scope, and the selection of oversight approach.

The goal has been to create a single compliance oversight design that represents an effective, repeatable and sustainable approach, whereby resources are aligned to the relative risks posed by an entity to the reliability of the bulk power system (BPS). The ERO is currently finalizing the documentation of the processes, procedures, and methodologies developed through the various pilots, and identified as best practices, to complete a single design for Inherent Risk Assessment (IRA) and Internal Control Evaluations (ICE). Documentation supporting IRA and ICE will be completed over the next two-months. A team is integrating the various approaches into a final design. The methodologies for IRA and ICE will be published with examples, demonstrating the application of the methodology. It is important to emphasize that we are not re-inventing anything. The practices associated with RAI, such as assessing risk and developing effective compliance oversight, are well established through a number of authoritative bodies.

¹ Generally Accepted Government Auditing Standards, The Institute of Internal Auditors International Professional Practices Framework, and The Committee of Sponsoring Organizations of the Treadway Commission: Internal Control – Integrated Framework

Next steps that will result in the full implementation of RAI by 2016 include: incorporating the processes into the 2015 Annual Implementation Plans and Actively Monitored List; developing and delivering training through the second half of 2014; deploying framework elements across the ERO Enterprise through 2015; and, conducting effective oversight to support full implementation by 2016.

Efforts continue regarding the formalization and documentation of the combined process and procedures developed through the pilots. Additionally, a final assessment of the uniform IRA and ICE approaches will be necessary to complete the evaluation process. The use of pilots has validated program design elements that are central to finalizing IRA and ICE and identified continued areas for development as well as activities necessary to assure a successful transition.

RAI Pilot Project Successes, Lessons Learned and Opportunities

Since February, a group of regional representatives (the development team) met to evaluate each pilot program in an effort to design and develop a common uniform risk-based approach. The development team presented the common framework and methodologies for assessing risk and evaluating controls to an evaluation team. Based on the design and information provided, the evaluation team noted the following successes:

- The RAI oversight plan framework provides a structure to uniformly apply processes across the ERO.
- The RAI oversight plan framework incorporates a flexible program design that can be applied based on a registered entities willingness to share management controls.
- The pilots clearly demonstrate that the assessment of risk creates a better oversight scope than the existing Actively Monitored List (AML).
- Better information can be obtained and evaluated through targeted and focused oversight and use of tools rather than through broad sweeping audits targeted at only assessing compliance for a prior period.

A simple example to illustrate the success of this approach comes from the Midwest Reliability Organization (MRO), which was able to more appropriately scope audits based on readily available information about selected registered entities. Basic risk elements that were evaluated included the registration function, facilities owned and/or operated, compliance history, general location of facilities, system information available in the public domain and, in one instance, the sharing of internal controls.

MRO applied the risk assessment methodology to three wind farms with the same registered function. Using the 2014 AML, MRO would have performed three audits, scoping 28 requirements (approximately 131 requirements apply to GO/GOPs). Through a review of risk elements, MRO developed an oversight strategy that considered the full set of requirements as they relate to the registered entities risk. Based on the risk assessment, MRO developed the following scope for each oversight approach:

- The first entity's scope consisted of 25 requirements, of which five of those requirements appear on the AML.
- The second entity's scope consisted of 20 requirements, again, five of the requirements appear on the AML.

- The third entity was scoped for two requirements, neither requirement appearing on the AML. Further, MRO used a self-certification to gather supporting data to assess compliance.

The value of evaluating core risk elements yielded a better scope, targeted at risk, with reasonable assurance of continued compliance in those requirements which pose the most risk to reliability. In this regard, the ERO Enterprise is finalizing the documentation of processes and methodologies that will be used to create examples and demonstrate the application of IRA and ICE.

While many aspects of the pilots were successful, efforts currently being undertaken by the ERO are a direct result of identifying opportunities for improvement. Specific opportunities include:

- Improving processes and procedures for obtaining and evaluating internal controls, specifically:
 - Defining the types of controls that help in assessing risk mitigation
 - Developing clear guidelines and examples demonstrating the extent and format of information necessary for a registered entity to explain and substantiate their controls
 - Providing training and clear examples for the ERO and industry related to the evaluation of internal controls
- The acquisition, analysis, and management of data is critical to the implementation of a risk-based compliance monitoring program:
 - Automated and centralized technical tool are going to be necessary for long term success and derive full efficiencies
 - Processes can be managed through tools such as excel but audit specific and data analysis specific tools will facilitate better efficiencies of process
 - Some regionally developed tools may support this but it will require additional evaluation

In addition to the successes and opportunities noted, there are two additional lesson learned regarding the impact to the use of audits as a primary oversight tool.

1. The implementation of a risk-based approaches has shown that other tools under the CMEP can be used more effectively in our goal of ensuring compliance with high value standards to reliability. For example, using more narrowly focused audits complimented by improved self-certifications and spot checks can provide better penetration in our oversight and normalize the compliance burdens of registered entities. One of the objectives of RAI was to match the right oversight tool (audit, spot check, or self-certification) with risk for effective compliance.
2. The pilots have clearly demonstrated that scoping will become more targeted and consider the effectiveness of controls around standards to substantiate compliance. And, the pilots have largely approached assessing risk in similar manner, further demonstrating that assessing risk is an established practice among those who have been trained or have the proper experience.

RAI Compliance Framework

The ERO oversight framework, the methodologies related to risk assessment and the evaluation of controls are grounded in generally accepted practices and internal control principles². While efforts are continuing regarding finalization of processes, procedures, and methodologies related to IRA and ICE, I would like to share some nuances related to the framework and ICE. The framework is designed to be flexible, assuring that it will not force a registered entity to submit to the assessment and testing of controls sooner than they are prepared. The IRA process for assessing risk is designed to work independently of the control evaluation (ICE) specifically for this purpose. Under professional practices, in the conduct of compliance oversight, although we are obligated to request internal control information from registered entities, they are not required to provide the information to us. Audit rules under the GAO and IIA are very specific on this matter. If registered entities provide internal control information to NERC and the Regional Entities, we are obligated to consider it in the scope of our compliance oversight. The IRA remains a beneficial process for appropriately scoping oversight activities based upon the inherent risks posed by the registered entity and selecting oversight methodologies based on the risks and activities applicable to their registered function(s).

Registered entities that choose to share their management practices and internal controls for evaluation in the determination of their oversight scope as well as testing, will proceed through the ICE process. The evaluation process for management practices and internal controls does not prescribe a design, compare designs, or determine the quality of one program versus another. Rather, the processes to perform an ICE takes into consideration that “no one size fits all”³ and allows each registered entity to tailor a control model to fit its needs. In this regard, ICE will establish a principled based approach for the evaluation of the necessary components in a system of internal controls. The primary factors that are being considered in the finalization of the evaluation and control testing design include:

- Does the control activity or combination of control activities mitigate the risk?
- Are the controls deployed through policies that establish expectations?
- Do procedures exist that put policies into action?
- Is there a design to determine if the components of the control are present and functioning?
- Do processes exist to evaluate and communicate non-compliance?
- Is there a process to take corrective action?

Finally, it should be noted that RAI does not replace the primary purpose of oversight activities, which is to determine compliance with the Reliability Standards and the associated requirements. Understanding risk and the controls designed to mitigate that risk allow the compliance staff to more thoughtfully select areas that should ultimately have the greatest impact on reliability.

Implementation Considerations

The RAI program was launched in early 2013 as the strategic initiative to transform the current compliance and enforcement program to one that is forward-looking, focuses on high reliability risk areas and reduces the administrative burden on registered entities. The ERO identified key compliance projects necessary to drive organizational alignment and create the foundation necessary to implement consistent risk based compliance

² ibid

³ FERC Policy statement on Compliance | October 16, 2008

methodologies and guidelines. The foundational projects consisted of creating a common annual CMEP Implementation Plan, developing and implementing an auditor checklist and auditor manual, adopting a single compliance auditor role expectations guide, and testing risk based methodologies through a series of pilots. The capstone project is finalizing the elements of RAI Oversight Plan Framework.

As we shift from the development and deployment of the common RAI approach, the NERC Regional Entity Assurance and Oversight department (Department) will be responsible for assisting with verifying the common implementation of RAI. Through the development of RAI, the Department has been transitioning from an organization that historically performed oversight of regional audits to an organization that will implement assurance and consulting methodologies. In this regard, the Department will:

- Develop and deliver training that sets expectation for compliance oversight processes and professional auditor conduct
- Consult with the Regional Entities on appropriate methodologies in the conduct of CMEP
- Deliver both mandatory and recommended guidance for CMEP performance to the Regional Entities
- Design and conduct broad based assessments and reviews to assure consistent application of the tools and methodologies developed for the CMEP work
- Identify process improvement opportunities and follow-up on corrective actions

While every effort is being made to develop and deploy a uniform approach for risk-based compliance monitoring, there are potential obstacles that must be monitored and managed appropriately. These include:

- Developing the procedures to assure replication across the regions in a consistent manner
- Assuring the right skill levels, competency and organizational structure to conduct the work without discrimination
- Managing a transition to new methodologies
- Assuring the timely development and deployment of training and verifying it is functioning
- Helping industry transition from paperwork compliance to demonstrating performance against Reliability Standards

Conclusion

In conclusion, while there is still much work to be done; NERC, the Regional Entities and our stakeholders, have shown a continued commitment to see this initiative be developed and implemented. We have established a solid foundation through the development and adoption of core tools like the auditor manual and working with industry to develop and disseminate materials outlining the project. We remain on target for the delivery of projects related to RAI and a fully implement program by 2016 to achieve the desired end-state of a fully functional risk-based approach to compliance monitoring. Thank you for the opportunity to appear before the Commission today.