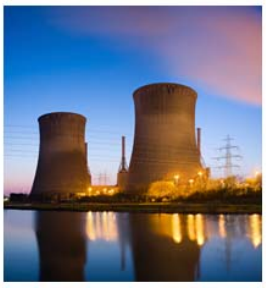
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Enterprise Guide for Internal Controls

Version 2

September 2017

RELIABILITY | ACCOUNTABILITY

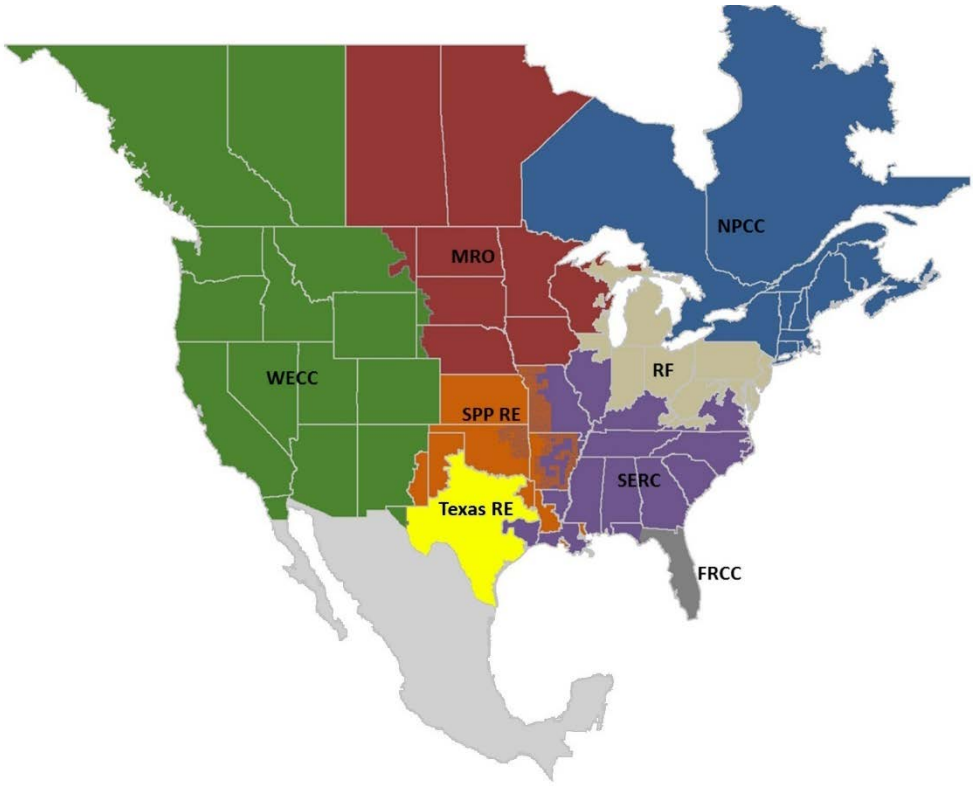
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the reliability and security of the bulk power system (BPS) in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the BPS through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the Electric Reliability Organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

The North American BPS is divided into eight Regional Entity (RE) boundaries as shown in the map and corresponding table below.



The highlighted areas denote overlap as some load-serving entities participate in one Region while associated transmission owners/operators participate in another.

FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
SPP RE	Southwest Power Pool Regional Entity
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

Effective internal controls support the reliability and security of the bulk power system (BPS) by identifying, assessing, and correcting issues; and their use can demonstrate reasonable assurance of compliance with NERC Reliability Standards. This ERO Enterprise Guide for Internal Controls describes the Electric Reliability Organization (ERO) Enterprise approach for understanding and assessing internal controls as part of the overall Risk-Based Compliance Oversight Framework (Framework).[1] This guide includes the ERO Enterprise approach for assessing internal controls during compliance monitoring activities. This guide also assists Compliance Enforcement Authorities (CEAs) in identifying and considering existing registered entity risk mitigation practices (commonly referred to as internal controls) in the development of the CEA's Compliance Oversight Plan (COP) for that particular registered entity.

The process for evaluating internal controls described herein applies to any type of registered entity regardless of size or function. As discussed, the internal controls evaluated relate to the inherent risk posed by a particular registered entity and any associated NERC Reliability Standards. Therefore, the extent of an evaluation and the application of the evaluation criteria will vary in accordance with the level of inherent risk posed by the registered entity.

Even effectively designed and implemented internal controls cannot provide absolute assurance of compliance with NERC Reliability Standards. The ERO Enterprise Guide for Internal Controls describes the approach CEAs use to assess the effectiveness of design and implementation of a registered entity's internal controls. It also accounts for the need to scale testing of internal controls to take into consideration the wide range of entity size and risk characteristics. The CEA develops a registered entity's COP following the process described in the ERO Enterprise Guide for Compliance Monitoring,[2] which considers results of internal control testing and other internal control information identified during Compliance Monitoring and Enforcement Program (CMEP) activities. The COP is dynamic, and CEAs may make modifications based on changes to the registered entity inherent risk assessment (IRA), internal controls, and performance considerations.

[1] Refer to the ERO Enterprise Overview of Risk-Based CMEP for additional information on the Risk-Based Compliance Oversight Framework.

[2] ERO Enterprise Guide for Compliance Monitoring

Revision History

Date	Version Number	Comments
December 2016	V1	• Renamed the "ICE Guide" to the *ERO Enterprise Guide for Internal Controls* • Incorporated approach for ERO Enterprise review of internal controls during CMEP activities • Revised and streamlined testing approach to focus on testing internal control design and implementation effectiveness • Included references to the *ERO Enterprise Guide for Compliance Monitoring* and content for COP development • Updated appendices ▪ Appendix A contains revised definitions ▪ Appendix B contains additional details around key controls
September 2017	V2	• Added series of principles to Section 1.0 - Internal Controls and Compliance Monitoring • Reordered Section 2.0 pertaining to the potential role of ICE to facilitate a general discussion about the value of evaluating internal controls before addressing Internal Controls Evaluations • Clarified process for sharing results in Section 3.1

1.0 Internal Controls and Compliance Monitoring

The ERO Enterprise follows professional auditing standards (e.g., Generally Accepted Government Audit Standards (GAGAS[3])) when conducting compliance audits and other CMEP activities.[4] Pursuant to such auditing standards, CEA staff will obtain an understanding of internal controls through inquiries, observations, inspection of documents and records, review of other CEA staff reports, and direct tests. The nature and extent of procedures CEA staff perform to obtain an understanding of internal controls may vary among compliance monitoring activities based on compliance monitoring objectives, inherent risk, known or potential internal control deficiencies, and the CEA staff's knowledge about internal controls gained in prior compliance monitoring activities.

A registered entity cannot be found noncompliant based on the internal control design or implementation unless there is a noncompliance with a requirement of the NERC Reliability Standards. A sound business approach to incorporating effectively designed and implemented internal control improves operational and compliance performance. Through evaluations, the CEA may take into account good governance practices of registered entities that effectively manage risk to BPS reliability. In addition, the lessons learned from evaluating internal controls may encourage the adoption of such practices throughout the ERO Enterprise and industry.

To fulfill the ERO Enterprise obligation to assure a highly reliable and secure BPS, the approach and processes for evaluating internal controls align with the following principles:

- Demonstrate reasonable assurance of a registered entity's ability to mitigate reliability risk
- Inform the risk-based approach for developing registered entity oversight and monitoring
- Focus on repeatability and sustainability to ensure reliability and security rather than administration to assemble and archive evidence

Effective controls provide value and help registered entities

- self-identify and mitigate reliability risks and compliance issues, which could lead to the ability to self-log and correct lower-risk issues as Compliance Exceptions rather than navigating through the full enforcement process;
- improve their reliability and security;
- inform the CEA's development of the registered entity's Compliance Oversight Plan (COP); and
- reduce the burden for audit preparation with a continuous monitoring process rather than a periodic event associated with the registered entity's preparation for compliance monitoring activity.

As described in the ERO Enterprise Guide for Compliance Monitoring[5], the ERO Enterprise recognizes that internal controls cannot provide absolute assurance of compliance with Reliability Standards. CEAs may modify the nature, timing, or extent of compliance monitoring activities based on their understanding and evaluations of internal controls. When developing or updating a registered entity's COP, internal controls may be used by the CEA to select appropriate compliance monitoring tools under the CMEP.

[3] GAGAS

[4] NERC ROP, Section 1207

[5] ERO Enterprise Guide for Compliance Monitoring

1.1 Understanding Internal Controls during CMEP Activities

As part of the CMEP process, CEA staff will obtain an understanding of internal controls during CMEP activities as well as during other registered entity interactions. The CEA's understanding of internal controls during CMEP activities, like a compliance audit, enable the CEA to make better-informed decisions around compliance and the registered entity's ability to sustain compliance and build reliability excellence. Additionally, a CEA's review of internal controls during CMEP activities can inform future monitoring and the COP.

After reviewing internal controls, the CEA should make decisions around the effectiveness of the design and implementation that may

- change the nature, extent, and timing of compliance testing during fieldwork or future fieldwork (e.g., audit fieldwork during a compliance audit);
- identify industry best practices, areas of concern, or recommendations; and
- refine the registered entity's COP and future compliance monitoring.

CEA staff should document decisions around the effectiveness of the controls. A registered entity's COP should take into consideration internal control information made available through CMEP activities like internal controls evaluations (ICEs), audits, spot checks, self-certifications, or mitigating activities.

2.0 Approach for Testing Internal Controls

The approach described within Section 2.0 applies to CEA assessments of internal controls during an ICE as well as during compliance monitoring activities. The range of assessment activities CEAs perform will vary based upon the registered entity's inherent risk (e.g., size and characteristics), selection and prioritization of internal controls for assessment, etc. CEAs follow the approach described within this guide and use professional judgment to select internal controls to assess and draw conclusions on the effectiveness of a registered entity's internal controls.

2.1 Major Inputs

A primary input into selecting internal controls to test is the results of a registered entity's IRA. During IRA development or refresh, the CEA identifies specific inherent risks and associated NERC Reliability Standards for the registered entity. The IRA identified risks that are relevant to an ICE. Additional inputs that may help identify controls to test include the following:

- ERO Enterprise and Regional Risk Elements
- The registered entity COP developed per the *ERO Enterprise Guide for Compliance Monitoring*
- Other registered entity information

Other information may include an initial list of internal controls for risk identified by the registered entity and applicable testing of those controls. CEAs may review some existing registered entity internal controls, focusing on reliability and security of the BPS and compliance with NERC Reliability Standards. CEAs do not expect registered entities to create additional documentation or evidence for purposes of a CEA's review of internal controls.

2.2 Evaluation of Design and Implementation

2.2.1 Internal Control Design

Design effectiveness involves evaluating an internal control as it relates to meeting an objective. A control will be less effective if there are missing attributes or the existing design does not meet its established objective. Internal controls should be commensurate with a registered entity's size and potential risk of the registered entity's operations to the BPS.

The CEA may obtain an understanding of internal control design through activities such as inquiries, observations, inspection of documents and records, work of others (e.g., internal audit departments), direct testing, etc. When a registered entity provides internal control information, the CEA may decide to perform a walkthrough to better understand and ensure an appropriate design. When evaluating internal control design, the CEA should use professional judgment to determine that it has sufficient and appropriate information to assess the effectiveness of the internal control design.[6]

Registered entities may use a variety of internal controls designed to provide reasonable assurance regarding the achievement of grid reliability, security of the BPS, and compliance with NERC Standards. Understanding the attributes or features of internal controls, including the types of internal controls (e.g., preventative, detective, corrective, or a combination of these) in place, helps the CEA better understand the internal control design and its linkage to NERC Reliability Standards objectives. Any internal control may fail, and a "perfect" internal control is not possible. In some cases, a CEA may determine that one particularly strong internal control provides

[6] The sufficient, appropriate evidence standard applies to the collection and review of information during an internal control review and evaluation, defined in GAGAS.

reasonable assurance of preventing or detecting noncompliance, but may determine in another case that a blend of internal controls is necessary.

An internal control cannot be effective if it is not effectively designed. During the design review, if the CEA decides that the internal control design is not capable of achieving an established objective(s) and addressing related risks, the CEA may determine not to review the internal control implementation. The CEA should document its design review, conclusions, and any feedback to the registered entity that it will share as described in Section 3.1.

2.2.2 Using the Work of Others

Many registered entities employ an independent team to assess compliance with their risk management strategy that includes adherence to NERC Reliability Standards. An independent internal control review may be conducted by a specialist, a government entity (such as the Government Accountability Office or Nuclear Regulatory Commission), a contractor who has been commissioned by the registered entity as a disinterested third party, or an internal department within the registered entity that is independent of the department performing Reliability Standards operations. If a registered entity seeks to have the CEA rely on the "work of others," the CEA team may review the independence, capabilities, and competencies of the individuals performing the review and any relevant documentation related to the assessment itself for consideration in updating a COP.

2.2.3 Internal Control Implementation

Implementation effectiveness includes an evaluation of whether the internal control is operating as designed. The implementation of an internal control is not effective if a properly designed control exists but does not operate as designed or if a person performing the control does not possess the necessary authority or qualifications to perform the control.[7]

When evaluating implementation effectiveness, the CEA will consider any supporting information that demonstrates implementation of the internal control. Based on the CEA's understanding of the internal controls, the CEA should determine whether they provide reasonable assurance of compliance with the identified NERC Reliability Standards. The CEA may have to review and test the implementation effectiveness for more than one internal control associated with a risk or NERC Reliability Standard.

Assessment Criteria

The CEA may use a binary effective/not effective method for assessing implementation effectiveness, or it may use a measured approach to assess internal control implementation. CEAs should have a documented methodology for assessing implementation, and this methodology may include, but is not limited to, the following:

- The automation of internal controls
- Compensating and supporting internal controls
- Registered entity identification of key controls
- The level of available internal control documentation
- Peer review of key controls within the registered entity
- Feedback on control design processes
- Registered entity's internal review and testing of existing internal controls

[7] GAGAS

2.2.4 Finalize Conclusions

The CEA should document conclusions around internal controls, including any control deficiencies noted during the assessment and provide documented feedback to the registered entity[8].

Internal control design deficiencies may include, but are not limited to, the following:

- An internal control necessary to meet the objective is missing.
- An existing internal control is not properly designed so that even if the control operates as designed, the control objective is not met.

Implementation deficiencies may exist, but are not limited to, when

- a properly designed control does not operate as designed; and
- a person performing the control does not possess necessary authority or competence to perform the control effectively.

CEAs may consider the following when making decisions around the overall effectiveness of internal controls and any deficiencies identified:

1. **The likelihood that the deficiency will result in a violation of a NERC Reliability Standard:** A deficiency means there is some likelihood a NERC Reliability Standard could be violated and the reliability of the BPS could be affected by the internal control failure. The greater the likelihood of violation, the greater the severity of the internal control deficiency, and the more likely that the associated NERC Reliability Standards shall be evaluated as per the IRA outcomes.
2. **The effectiveness of other internal controls:** The effective operation of other internal controls may prevent or detect a risk to reliability. The presence of other controls may provide support for reducing the severity of a deficiency and the associated monitoring of relevant NERC Reliability Standards.
3. **The aggregating effect of multiple deficiencies on NERC Reliability Standard compliance:** A combination of internal control deficiencies may adversely affect the registered entity's ability to comply with one or more NERC Reliability Standards, and affect the reliability of the BPS, depending on the objectives of the internal controls.

Key questions for finalizing conclusions should address the following:

- Do the internal controls mitigate the risks identified in the IRA?
- If the internal controls do not completely mitigate the risk, should correction be encouraged, rather than testing of individual NERC Reliability Standards?
- How do the entity's internal controls inform the COP for this registered entity?

2.2.5 Outcome

The evaluation outcome of internal controls includes the following:

- A list of the assessed internal controls and the decisions regarding design and implementation effectiveness
- Internal control decisions that inform the registered entity's COP and changes to the nature, extent, or timing of assessing compliance with NERC Reliability Standards

As the CEA prioritizes risk areas associated with any individual internal control deficiencies, focus must be kept on tailoring the COP for the registered entity. An internal control that the CEA determines to be deficient in some

[8] GAGAS

manner does not mean a NERC Reliability Standard has been or will be violated. A deficient internal control may simply result in the CEA modifying its compliance monitoring of the registered entity. The CEA shall prioritize the remaining risks based upon the entity's internal controls. The CEA will adjust the COP to examine NERC Reliability Standards not effectively protected by an internal control.

2.3 Reviews and Retests of Internal Controls

CEAs should review and revise assessments of internal controls as new, emerging, or unique information is obtained and as significant changes to the registered entity occur. As such, the CEA may review and retest internal controls previously evaluated to ensure the facts and circumstances remain the same and assessments are still appropriate. Triggers for conducting a review may include, but are not limited to, changes in organizational structure, changes in internal control programs, changes in registered entity performance (e.g., misoperations, system events, or any new violations identified), and feedback from CEA staff or CMEP activities. For example, if a merger occurs between registered entities, the merger may impact internal control design and implementation that would require additional testing to determine effectiveness.

2.4 Internal Controls Evaluation

As described in the Framework, registered entities have an opportunity to: 1) provide, on a voluntary basis, information to their respective Regional Entity about their internal controls that address the risks applicable to the entity and for identifying, assessing, and correcting noncompliance with Reliability Standards; and 2) demonstrate the effectiveness of such controls.

2.4.1 ICE Objective

The primary objective of ICE is to review internal controls to obtain reasonable assurance that their design and implementation better ensure compliance with Reliability Standards. ICE supports more informed decisions on compliance monitoring (i.e., develop COPs or modify nature, extent, and timing of testing of compliance), facilitates selection of tailored CMEP tools, and provides direction on continuous improvement for the registered entity.

The CEA is ultimately responsible for determining whether a registered entity has internal controls that provide reasonable assurance of compliance with NERC Reliability Standards. The CEA makes this determination by understanding the BPS risks the registered entity is susceptible to and understanding how the registered entity manages or mitigates those risks.

2.4.2 ICE Timing and Selection of Internal Controls

The ICE process involves collaboration and coordination between the CEA and a registered entity. CEAs typically conduct an ICE outside of a compliance monitoring activity. The CEA will work with the registered entity to determine the timing of ICE activities. For example, an ICE may occur prior to a scheduled compliance audit to help refine the scope of the audit or inform testing of compliance with NERC Reliability Standards during the audit. As another example, an ICE may occur after a compliance audit if the registered entity and CEA have identified internal controls that could inform future compliance monitoring and the COP.

CEAs may select and prioritize internal controls to test their effectiveness. For example, CEAs may use the ERO or RE Risk Elements, Regional Risk Assessments, and IRA results to prioritize the testing of internal controls. CEAs can also coordinate with a registered entity to determine which internal controls are available for testing, identify possible key internal controls, or determine whether the registered entity has certain internal controls that may be more mature and more appropriate for testing.

ICE is a voluntary process, and registered entities, regardless of size, may participate in an ICE. The complexity of internal controls will vary across registered entities, and the CEA evaluation of such internal controls will be adjusted according to the registered entity's BPS risk.

3.0 Results Documentation

CEAs should follow established documentation protocols, such as the NERC Rules of Procedure (ROP), and use professional judgment to determine documentation needs throughout the review of a registered entity's internal controls during monitoring engagements as well as ICE. The extent of the documentation is directly linked to the 1) nature and complexity of the internal controls reviewed; 2) procedures performed; and 3) methods and technologies used during the process. The more significant and complex these factors are, the greater and more detailed the documentation should be.

The CEA shall maintain documentation that clearly demonstrates its decisions around internal controls review as well as ICE. Documentation includes all data and information obtained, reviewed, and tested.

3.1 Sharing Results

During internal control reviews, either as part of a monitoring engagement or ICE, the CEA will hold discussions with registered entities to understand the design and implementation of internal controls and the effectiveness of such internal controls. CEAs should facilitate a collaborative dialogue with the registered entity throughout the internal controls review. As needed, CEAs should work with the registered entity to ensure the CEAs have sufficient information to make decisions on the effectiveness of internal controls and to determine how they may influence changes to the registered entity's COP.

The CEA should provide feedback to the registered entity on internal controls, such as recommendations for improvements, discussions around best practices, areas of concerns, etc.

The CEA will document and communicate its decisions and conclusions around internal controls and any COP updates to the registered entity. The CEA will share changes to the COP no later than the notification periods required by the NERC ROP for selected CMEP tools, and CEAs will provide additional information on compliance monitoring activities in the annual *ERO Enterprise CMEP Implementation Plan*.

3.2 Documentation Retention

The CEA will retain all relevant documentation demonstrating the nature and extent of information reviewed, the procedures performed, and conclusions reached. Documentation that should be retained includes (but may not be limited to) analyses, memoranda, summaries of significant findings or issues, checklists, abstracts, copies of important documents, and paper or electronic correspondence concerning significant findings or issues. Additionally, finalized narrative descriptions, questionnaires, checklists, and flowcharts created through the internal controls testing are also considered important documentation and should be retained.

When determining the nature and extent of documentation that should be retained, the CEA should consider the information that would be required for a prudent auditor who was not involved with the internal control assessment to understand the work performed and the conclusions reached during internal control testing. CEAs should maintain supporting documentation for review by NERC in connection with NERC's oversight of the compliance assurance program.

CEAs should also follow the NERC ROP, as well as ERO Enterprise and RE processes as they apply to handling confidential information and data retention periods.

4.0 References

Below is a list of reference materials that support the basic principles, concepts, and approaches within this guide. CEAs use these reference materials to assist in implementing the Framework and processes detailed in this guide. These reference materials identify 1) where and to what extent professional judgment should be applied; 2) the sufficiency and appropriateness of evidence to be examined; and 3) the sufficiency and appropriateness of the documentation required. Additionally, NERC ROP and key Federal Energy Regulatory Commission (FERC) filings and orders contain descriptions of the Framework discussed in this guide.

- Generally Accepted Government Auditing Standards (GAGAS), located at: http://www.gao.gov/yellowbook/overview
- ERO Enterprise CMEP Manual, located at: http://www.nerc.com/pa/comp/Pages/ERO-Enterprise-Compliance-Auditor-Manual.aspx
- Annual ERO Enterprise CMEP Implementation Plan, located at: http://www.nerc.com/pa/comp/Resources/Pages/default.aspx
- NERC ROP, located at: http://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx
- Key FERC filings and Orders:
  - Informational Filing of NERC Regarding Implementation of the Reliability Assurance Initiative (November 3, 2014)
    - FERC Order on Risk-Based Compliance Monitoring and Enforcement Program (February 19, 2015)
  - Compliance Filing of NERC and Petition for Approval of Rules of Procedure Revisions (July 6, 2015)
    - Order Conditionally Accepting CMEP Compliance Filings and ROP Revisions (November 4, 2015)[9]
  - Annual Compliance Monitoring and Enforcement Program Report (February 18, 2016)
    - Letter Order Accepting Annual CMEP Report (April 14, 2016)

[9] FERC's November 4 Order directed NERC to revise the applicable Rules of Procedure to reflect certain components of the Risk-Based CMEP, specifically related to enforcement activities of self-logging and Compliance Exceptions. Therefore, related filings and Orders are not appropriate for this guide.

Appendix A: Considerations for Understanding Control Design

Using Key Controls to Prioritize Testing

When evaluating controls, CEAs will obtain information to understand how the registered entity designs and manages internal control activities to mitigate identified risks. Additionally, potential failure modes of an internal control program need to be understood along with understanding what detection methods are deployed to identify potential failures of internal controls. Although every internal control may be important to the internal control program, some internal controls are more relevant to monitor than others in supporting a conclusion that the internal control program (or any portion of such program) is effective.

To help prioritize or identify which controls should be reviewed, the CEA may coordinate with the registered entity to understand the controls in place as well as any key controls that could impact testing. Key internal controls may include those that represent the most likely point of failure regarding significant risks identified during the IRA. For example, if patch management were to be identified as a significant inherent risk for an entity, a failure point for this risk could be that the entity was not aware of the availability of a security patch, potentially leading to a subsequent failure to assess, test, and install that security patch. To prevent this failure, a CEA may consider implementing a key internal control such as an automated alert or notification system that advises the entity's security personnel of the availability of a security patch. Such an alert would reduce the likelihood the entity would fail to assess, test, and install the security patch.

The CEA should examine the interactions between internal control activities to identify additional key internal controls. Individual internal controls often do not address a risk completely by themselves. Some internal controls may be identified as key because their operation can prevent other control failures or detect and correct control failures before they become significant to an organization. Often, multiple internal controls, together with other components (such as control environment, risk assessment, etc.), should be considered to address a risk identified during the IRA.

The CEA should also consider how various departments and organizational levels are impacted by the risk highlighted in the results of IRA process. The CEA might need to determine the organizational level, locations, or business units at which to perform testing for key internal controls. Conversely, the CEA might choose not to evaluate locations or business units not impacted by the highlighted risks. The goal is to identify those internal controls that, when monitored, will provide reasonable assurance that the overall internal control program is working effectively and efficiently. Especially in a small-to-medium-sized organization, an internal control for "training" may apply to the entire organization, and thus the CEA may test the "training" internal control in lieu of testing the many NERC Reliability Standards and Requirements. Conversely, in a large organization, a single type of power plant may be susceptible to an identified risk. It makes sense to test only those affected plants for internal controls associated with a particular risk, as the entire organization may not need those specific single internal controls to operate effectively.

The identification and selection of key internal controls can be facilitated by considering factors that increase the risk that the internal control program will fail to properly manage or even mitigate a given risk. Factors may include complexity, judgment, manual versus automated internal controls, and known control failures. Reasonable people might reach different conclusions on which internal controls are key and which are not. The varying nature of risk and internal controls can lead two organizations to implement internal controls and monitoring procedures differently.

Appendix B: Definitions

Compliance Oversight Plan (COP): A plan consisting of the oversight strategy for a registered entity, including the list of Standard requirements for monitoring, the CMEP tool to be used, and the interval of monitoring.

Corrective Internal Control: An internal control designed to fix a problem that may have arisen.

CMEP Tools: In context of this guide, the compliance monitoring processes that comprise a CEA's COP. CMEP tools are described in Section 3.0 of the NERC Rules of Procedure, Appendix 4C, and include but are not necessarily limited to, compliance audits, spot checks, self-certifications, and periodic data submittals.

Detective Internal Control: An internal control designed to identify errors or deviations from the norm.

Inherent Risk Assessment (IRA): A review of potential risks posed by an individual registered entity to the reliability of the bulk power system (BPS).

Internal Control: In the context of the risk-based compliance oversight framework, internal controls are the processes, practices, policies or procedures, system applications and technology tools, and skilled human capital an entity employs to prevent, detect, and correct noncompliance with Reliability Standards and address risks associated with the reliable operation of its business. Examples may include oversight, risk assessment, control activities, communications, training, and monitoring. Internal controls may operate at an entity or organizational level, as well as an activity or process level.

Key Internal Control: Internal controls that most effectively and efficiently achieve the control objectives and can be used to prioritize or focus testing when evaluating overall effectiveness of internal controls.

Preventive Internal Control: An internal control designed to avoid an unintended event or consequence.

Professional Judgment:[10] CEA staff use professional judgment in planning, performing, and reporting results of CMEP activities. Professional judgment represents the application of the collective and individual knowledge, skills, and experiences of all the personnel involved with a CMEP activity. In addition to personnel directly involved in the audit, professional judgment may involve collaboration with other stakeholders, external specialists, and management in the audit organization.

Reasonable* Assurance: Conclusions based on evidence that is sufficient and appropriate to support the CEA's conclusions. **Note: Emphasis on "reasonable", not "complete" or "absolute" assurance.*

Walkthrough: A procedure used during an evaluation of an entity's internal control to gauge the effectiveness of an internal control. A walkthrough traces a process step-by-step from its inception to the final disposition.

[10] GAGAS