

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

ERO Enterprise

Guide for Internal Controls

December 2025

RELIABILITY | RESILIENCE | SECURITY



Table of Contents

Preface iii

Statement of Purpose iv

Chapter 1: Internal Controls and Compliance Monitoring 1

 Understanding Internal Controls during CMEP Activities 1

 Global (Entity-Wide) Internal Controls..... 2

Chapter 2: Internal Controls Assessment Approach..... 3

 Major Inputs for Selecting Internal Controls to Assess 3

 Capturing Internal Controls During CMEP Activities 3

 Assessment of Design and Implementation..... 3

 Internal Control Design..... 3

 Internal Control Implementation and Effectiveness 4

 Using the Work of Others..... 4

 Reviews and Reassessments of Internal Controls 5

Chapter 3: Sharing Results 6

Chapter 4: References..... 7

Appendix A: Key Terms, Definitions, and Concepts 8

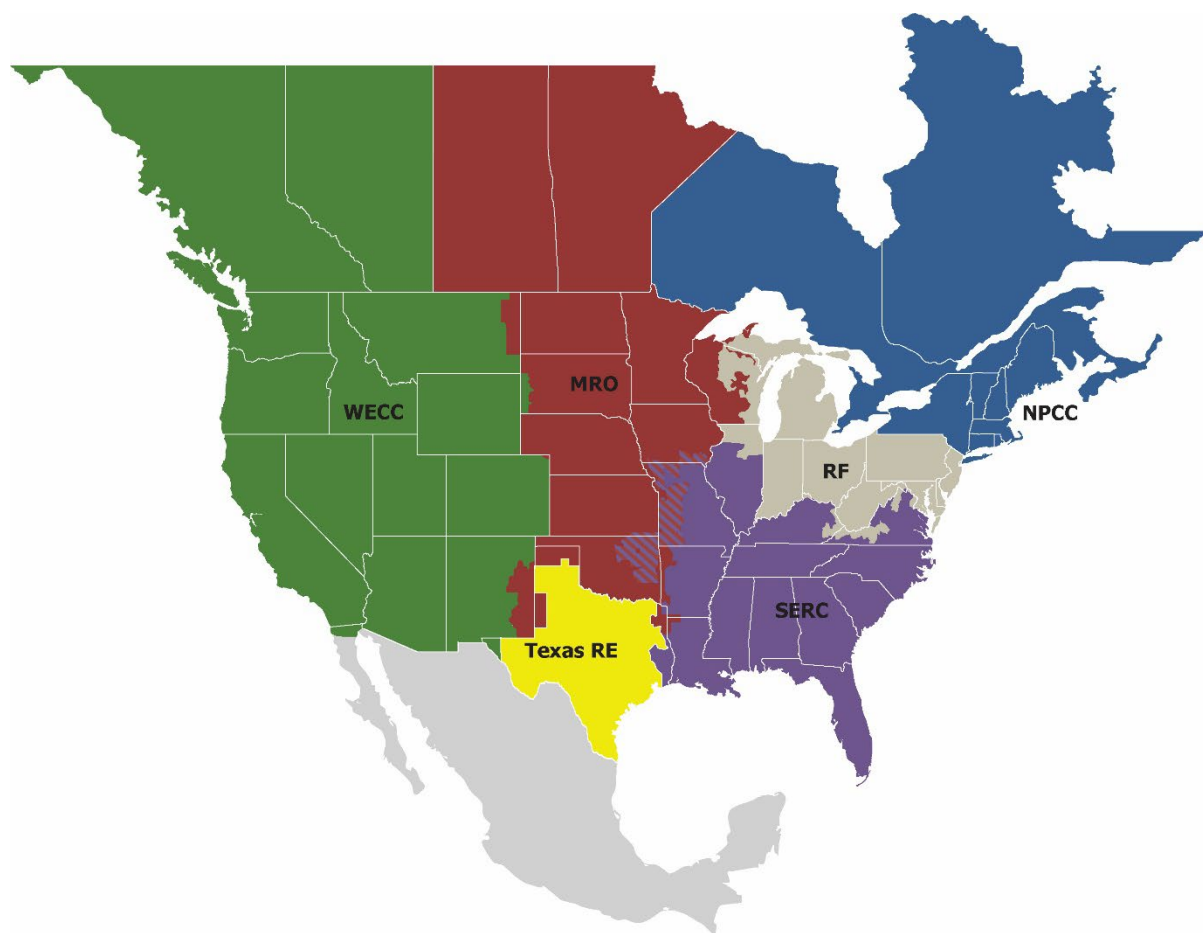
Revision History..... 10

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of NERC and the six Regional Entities, is a highly reliable, resilient, and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six Regional Entities as shown on the map and in the corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Statement of Purpose

Effective internal controls support the reliability and security of the BPS by identifying, assessing, and correcting issues; and their use can demonstrate reasonable assurance of future compliance with NERC Reliability Standards.

The *ERO Enterprise Guide for Internal Controls* describes the ERO Enterprise approach for understanding, assessing, and monitoring internal controls as part of the overall risk-based compliance monitoring and enforcement process.

The process for assessing internal controls described herein applies to any type of registered entity regardless of size or function. The internal controls assessed relate to a registered entity's inherent risk associated with BES reliability and security risk. Therefore, the extent of an assessment and the application of the assessment criteria will vary according to the level of inherent risk posed by the registered entity.

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 Compliance Enforcement Authorities (CEA) use to assess the design, effectiveness, 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.

Chapter 1: Internal Controls and Compliance Monitoring

The ERO Enterprise follows professional auditing standards (e.g., Generally Accepted Government Audit Standards (GAGAS)) when conducting compliance audits and other Compliance Monitoring and Enforcement Program (CMEP) activities. 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, or direct tests. The nature and extent of procedures CEA staff use 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, or the CEA staff's knowledge about internal controls gained in prior compliance monitoring activities.

A sound business approach to incorporating effectively designed and implemented internal controls improves operational and compliance performance. Through assessments, the CEA may consider good governance practices of registered entities that effectively manage risk to BPS reliability. In addition, the lessons learned from assessing internal controls may encourage the adoption of such practices throughout the ERO Enterprise and industry.

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

- Internal controls demonstrate reasonable assurance of a registered entity's ability to mitigate reliability risk in the future.
- Internal controls are reviewed in the audit process and may affect the registered entity oversight and monitoring.
- Assessments focus on repeatability and sustainability to ensure the reliability and security of the BES rather than administrative processes implemented to assemble and archive evidence.
- A registered entity cannot be found non-compliant based on the internal control design or implementation unless there is a noncompliance with a requirement of the NERC Reliability Standards.

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 reliability and security;
- provide CEAs with details required for the development of Compliance Oversight Plans (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.

CEAs may modify the nature, timing, or extent of compliance monitoring activities based on its understanding and assessments 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. As described in the *ERO Enterprise Guide for Compliance Monitoring*, the ERO Enterprise recognizes that internal controls cannot provide absolute assurance of compliance with Reliability Standards.

Understanding Internal Controls during CMEP Activities

As part of the CMEP program, 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, enables the CEA to make better-informed decisions about a 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, Positive Observations, Areas of Concern, or Recommendations; and
- refine the registered entity's COP and future compliance monitoring.

Global (Entity-Wide) Internal Controls

Internal controls may be considered "Global" or "Entity-Wide" (organizational) as well as "activity level" (operational) controls. The following concepts are helpful to understand the extent of development of a registered entity's global internal controls program:

- Global internal controls generally apply across an organization and may function in a complementary manner alongside operational internal controls.
- Examples of global controls may be reflected in a registered entity's Risk Management program or, for example, a registered entity's compliance department comprehensive tracking system that addresses all Standards and Requirements that apply to the registered entity.
- An example of operational level controls may be internal controls designed to reduce the risk of noncompliance with a specific Standard and Requirement, and/or an area of risk associated with a specific Standard and Requirement.

Chapter 2: Internal Controls Assessment Approach

CEAs use professional judgment to select risks in which to focus and draw conclusions about the effectiveness of a registered entity's corresponding internal controls. The range of assessment activities CEAs perform will vary based on the registered entity's risk.

Major Inputs for Selecting Internal Controls to Assess

Internal controls are selected for assessment based on an entity's residual risk. The CEA identifies risks that are relevant to the entity and serves as key talking points during discussions throughout the engagement. Inputs that may help identify controls to test include:

- Inherent risk
- ERO Enterprise and Regional Risk Elements
- The registered entity COP
- Reliability Assessments Performance Analysis and Event Analysis (RAPA and EA)
- Other registered entity information, such as risk associated with historical PNC root causes and common failure points.

Capturing Internal Controls During CMEP Activities

During CMEP activities like audits, spot checks, or self-certifications, the CEA will request and assess internal controls that work to mitigate identified prioritized risks. While the CEA will likely request a copy of evidence of any process documents that mitigate the risks and concerns being addressed in the CMEP activity, the registered entity may also wish to volunteer additional internal controls for assessment and documentation outside of the prioritized risks.

In the absence of any process documents, the CEA may request a description via a request for information (RFI) or interviews.

Assessment of Design and Implementation

Internal Control Design

Design effectiveness involves assessing internal controls as it relates to meeting an 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 assessing 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. This may include considerations such as:

- Is the activity covered by the control performed frequently, periodically, or rarely?
- Is the activity performed manually or is it automated?
- Does the control address:
 - potential human performance issues?
 - identified failure point(s)?

- Does the control include segregation of duties between personnel responsible for performing the control?
- Does the control include Quality Assurance/Quality Control (e.g., one person performs a task, and another person is responsible for verifying the task was performed or one person fills-in a form, and another person verifies the form was completed correctly)?

Registered entities may use a variety of internal controls designed to achieve and maintain grid reliability, secure the BPS, comply with NERC Standards, and decrease the overall risk to the BPS. Understanding the attributes or features of internal controls, including the types of internal controls (e.g., preventative, detective, corrective, or a combination of these), helps the CEA better understand the internal control design. 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 reasonable assurance of preventing or detecting noncompliance but may determine in another case that a blend of internal controls is necessary.

Internal control design is deficient when the objective cannot be met by the internal control, or the control only partially achieves the objective.

Internal Control Implementation and Effectiveness

Implementation effectiveness includes an assessment 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.

When assessing implementation effectiveness, the CEA will consider any supporting information that demonstrates the implementation of the internal control. A description of the control activity alone, without examples of supporting evidence, will not suffice to rank the control as effective.

Measures of effectiveness may include demonstrated performance observed during the audit, SME competency during an inquiry, and a “live” re-performance of controls, and any tools/applications used, for the audit team. Considerations in reviewing effectiveness may include:

- Has the extent to which the controls reduce risks been assessed?
- Are the controls implemented as they were designed?
- Do the controls, as implemented, appear to be effective in reducing the risk?

Using the Work of Others

Registered entities may employ an independent team to assess compliance with their risk management strategy which 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), 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.¹

¹ The ERO Enterprise CMEP Practice Guide - Using the Work of Others is located on the NERC website at: <https://www.nerc.com/globalassets/programs/compliance/compliance-guidance/cmep-practice-guides/cmep-practice-guide---using-the-work-of-others.pdf>

Reviews and Reassessments of Internal Controls

CEAs may review and revise assessments of internal controls based on new, emerging, or unique information such as 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 reassessment to determine continued effectiveness.

Chapter 3: Sharing Results

During internal control reviews as part of a monitoring engagement, 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 engagement. 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, Positive Observations, Areas of Concern, etc. The CEA's review of internal controls will be used to inform the future COP report.

Chapter 4: References

Below is a list of reference materials that support the basic principles, concepts, and approaches within this guide. As part of the assessment methodology, the ERO references existing internal control frameworks to promote a common language that will help conversations across ERO staff in addition to conversations with registered entity staff. These frameworks include the GAO Yellow Book, GAO Green Book, and the COSO Framework, all of which include common key terms and cross-references.

- GAO Green Book – “5 Components and 17 Principles of Internal Control”
- GAO Green Book – Figure 2 – “Achieving Objectives through Internal Control”
- GAO Yellow Book Chapter 8 – Section entitled “Assessing Internal Control”
- COSO Internal Control Integrated Framework – Five components of “The Cube”
 - Control Environment
 - Risk Assessment
 - Control Activities
 - Information and Communication
 - Monitoring Activities
- Other Frameworks
 - Carnegie Mellon Capability Maturity Model

Appendix A: Key Terms, Definitions, and Concepts

The following key terms, definitions, and concepts are blended from the relied-upon established frameworks, in addition to ERO-specific key terms (e.g., within the NERC CMEP Manual).

Area of Concern – A situation that, if not addressed, could develop into future noncompliance or risk to the BPS. Ineffective or nonexistent internal controls may contribute to an Area of Concern.

Component (Green Book Principle 12, which acknowledges COSO) – One of the five required elements of internal control. The internal control components are Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring

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.

Control Activities (Yellow Book Paragraph 10.02) - The policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the entity's objectives and address related risks.

Control Environment – Control Environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The board of directors and senior management establish the tone at the top regarding the importance of internal control including expected standards of conduct.

Control Objective (Green Book Glossary) - The aim or purpose of specified controls to effect relevant principles within each component of internal control (paragraph OV3.05).

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

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

Failure Points (WECC/ERO) – Concepts and/or activities that might lead to failure of control design or implementation, which could lead to risk of noncompliance or operational risk.

Global / Entity-Wide Internal Controls (ERO) – Internal controls designed to meet entity-wide objectives, which are broader and/or not limited to IC designed to meet objectives specifically related to Standards and Requirements

Green Book - The commonly used name for Standards for Internal Control in the Federal Government

Inherent risk (Green Book Glossary) - The risk to an entity in the absence of management's response to the risk (paragraph 7.03)

Inherent risk - The risk that exists *prior to* the implementation of internal controls (consistent with Green Book definition) – check manual p. 232 glossary.

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 (Yellow Book paragraph OV1.01) - A process affected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved.

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

Monitoring Activities (COSO Principle) – Monitoring activities are periodic or ongoing evaluations to verify that each of the five components of internal control, including the controls that affect the principles within each component, are present and functioning.

Positive Observation –A conclusion reached during an audit that relates favorably with respect to the quality of the registered entity's processes, controls, or corporate culture of compliance.

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

Process –A process (or method or function) is a collection of related, structured activities or tasks in which a specific sequence produces a service or product (serves a particular organizational goal). A process can also be referred to as a business process or operational process.

Professional Judgment –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.*

Recommendation –Suggested improvements in the compliance program, control-related processes, procedures, or tools to enhance the reliability, security, or resiliency of the BES. Opportunities for process improvements should be shared with the Registered Entity.

Residual risk (Green Book Glossary) - The risk that remains after management's response to inherent risk (paragraph 7.03).

Risk (Green Book Glossary) - The possibility that an event will occur and adversely affect the achievement of objectives (paragraph 7.02).

Revision History

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 <i>ERO Enterprise Guide for Compliance Monitoring</i> 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
December 16, 2025	V3	• Major Revision removing all references to ICE and the ICE process • Removed Appendix containing additional details around key controls • Review to ensure alignment with Joint Monitoring Activities.