NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Enterprise Internal Control Evaluation Guide

October 2014

RELIABILITY | ACCOUNTABILITY



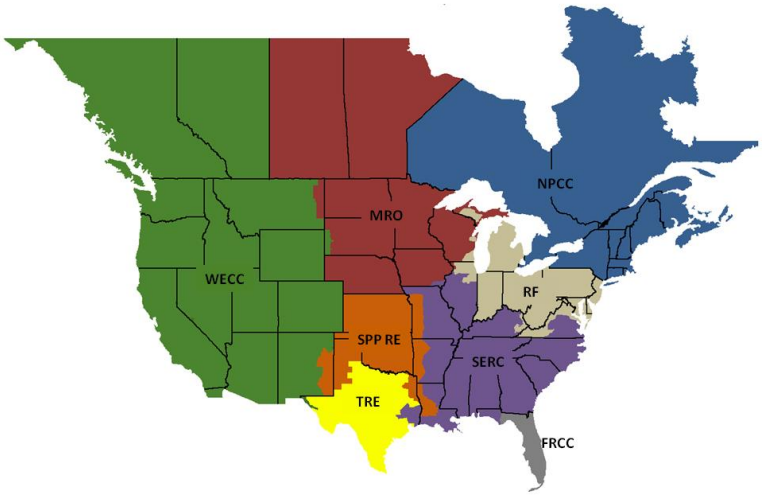

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to ensure the reliability 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 several assessment areas within the eight Regional Entity (RE) boundaries, as shown in the map and corresponding table below.



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
TRE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This Guide describes the common ERO Enterprise process for evaluating internal controls. Many elements described in this Guide may be part of current compliance monitoring activities. This Guide will assist Compliance Enforcement Authorities (CEAs) in identifying and more effectively considering existing registered entity risk mitigation practices (commonly referred to as internal controls) in the development of the CEA's oversight plan for that particular registered entity. The internal control evaluation (ICE) process is part of the overall Risk-Based Compliance Oversight Framework (Framework). [1]

NERC oversight of all components of the Framework will be essential to the proper application of the Framework over the long-term. With the completion of the design, reflected in the various guides published, and the baseline training provided to ERO Enterprise staff, the Framework is ready to be implemented. Over time, and through NERC's oversight of the program, areas that require additional guidance and training will be identified and addressed (either in the form of revised guides or through other means). In identifying such areas, NERC will consider the feedback from registered entities, Regional Entities, and other stakeholders. This iterative review cycle provides the most effective means of quickly adapting to specific implementation challenges.

The ICE is a voluntary process that is used to further determine the focus and selection of appropriate tools to be used by CEAs under the Compliance Monitoring and Enforcement Program (CMEP).[2] In an effective program, an entity's internal control components work together to provide reasonable assurance to achieve an organization's objectives, which, for purposes of this Guide, refer to compliance with mandatory NERC Reliability Standards.

A good internal control program improves operational and compliance performance. Through the ICE process, the CEA may take into account good governance practices of registered entities that reduce BPS reliability risks. In addition, the ICE process may encourage the adoption of such practices throughout the ERO Enterprise.

The process for evaluating internal controls described in this Guide can be used on small, medium, and large entities. As discussed in the Guide, the controls to be evaluated pursuant to the ICE process are those related to the inherent risk posed by a particular registered entity. Therefore, the extent of an evaluation and the application of the evaluation criteria will naturally vary in accordance with the level of inherent risk posed by the registered entity.

Even an effectively designed and implemented internal control program cannot provide absolute assurance of compliance with NERC's Reliability Standards. This Guide describes a method that can be used to evaluate the design and effectiveness of an entity's internal control program to support the creation of an effective compliance oversight plan, recognizing the need to appropriately scale the internal control evaluation to take into account the wide range of entity size and risk characteristics. If an entity chooses to not provide internal controls information, the CEA will use the results of the IRA to scope the entity's compliance oversight plan.

Revision History

Date	Version Number	Comments

[1] See [LINK] for a complete discussion of the Compliance Oversight Framework. As part of the Framework, CEAs will review their registered entities' risk posture periodically through the processes outlined in the Inherent Risk Assessment (IRA) Guide [LINK]. After this review, the registered entity will have the opportunity to provide information concerning their internal controls to focus the scope of their Compliance Oversight Plan.

[2] The CMEP is Appendix 4C of the NERC Rules of Procedure.

1.0 Internal Control Evaluation

1.1 ICE role within the overall Risk-based Compliance Oversight Framework

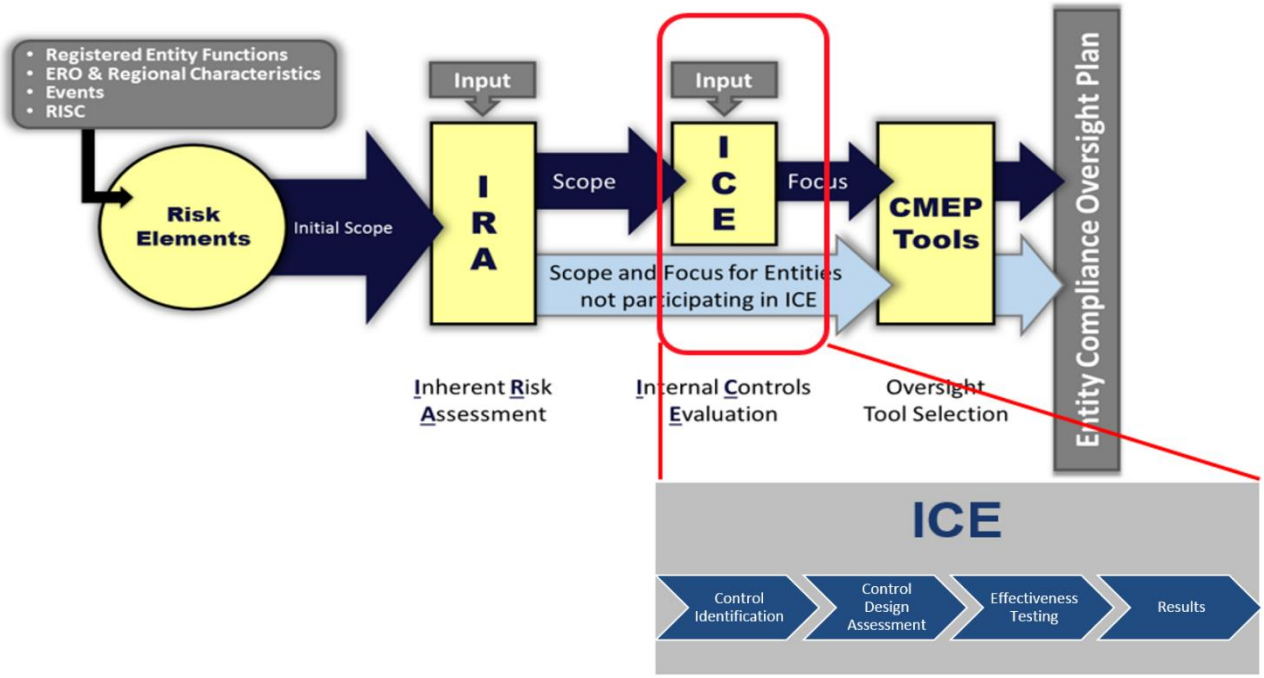


Figure 1: Risk-based Compliance Oversight Framework

1.2 Major inputs into the ICE

When a registered entity undergoes an inherent risk assessment, the CEA identifies specific risks (and associated Reliability Standards) to which the registered entity is susceptible. Only those risks (and associated NERC Reliability Standards and Requirements) are relevant to an internal control evaluation.

1.2.1 Inputs from the Inherent Risk Assessment

- Inherent risks to the reliability of the BPS (including those risks specific to individual Regional Entity footprints) applicable to the registered entity.
- List of prioritized NERC Reliability Standards and Requirements addressing the inherent risks.
- Relevant information including assumptions used during the IRA decision making process.
- Draft compliance oversight plan for the registered entity.
- Entity information gathered in response to results of the IRA, including initial list of controls and/or applicable testing of controls provided by the registered entity.

Internal controls are selected for testing based upon an entity's inherent risk, as determined through the process described in the IRA Guide. Only those controls that impact such risks will be considered during the ICE process.

1.3 Objectives of the ICE

The primary objective of the ICE is to focus the compliance oversight efforts of the CEA by recognizing the internal controls a registered entity employs to manage reliability risks. The CEA is ultimately responsible for determining whether a registered entity has implemented an internal control program containing sufficient controls that provides reasonable assurance of compliance with Reliability Standards in the service of reliability. The CEA will make this determination by understanding the BPS risks to which the registered entity is susceptible and understanding how the registered entity manages or mitigates those risks. This process can be used on small, medium, and large-sized entities. The complexity of internal controls and the CEA evaluation of such internal controls will be scaled in accordance with the size of the registered entity, as described in this Guide.

For example, smaller entities are likely to have less layers of management, and thus may have less complex and broader reaching internal controls that are more likely to span an entire organization, across many NERC Reliability Standards and Requirements, and the CEA may take into account that large span of controls.[3] Likewise, the CEA may be able to conclude that the smaller entity's simple controls (e.g., relevant policies and procedures, with compliance confirmed through management reports and supported by a culture of compliance emanating from an internal compliance program) are effective and reasonable relative to the size of the entity, its registrations, and the risk it poses to the BPS.

When the CEA has reasonable assurance that internal controls are functioning to protect reliability, detailed testing of documentation supporting compliance with those individual NERC Reliability Standards and Requirements associated with those internal controls may not be necessary.

[3] For instance, a smaller entity may have one internal control program for "maintenance" that covers FAC-003, PRC-005, PRC-008, PRC-011, PRC 017 and numerous other operational and regulatory requirements. The CEA may be able to test that one maintenance internal control program instead of testing each of these NERC Reliability Standards and Requirements

2.0 ICE Overview

This Guide focuses on three key areas in the application of ICE by the CEA. Figure 2 below illustrates the overall ICE process.

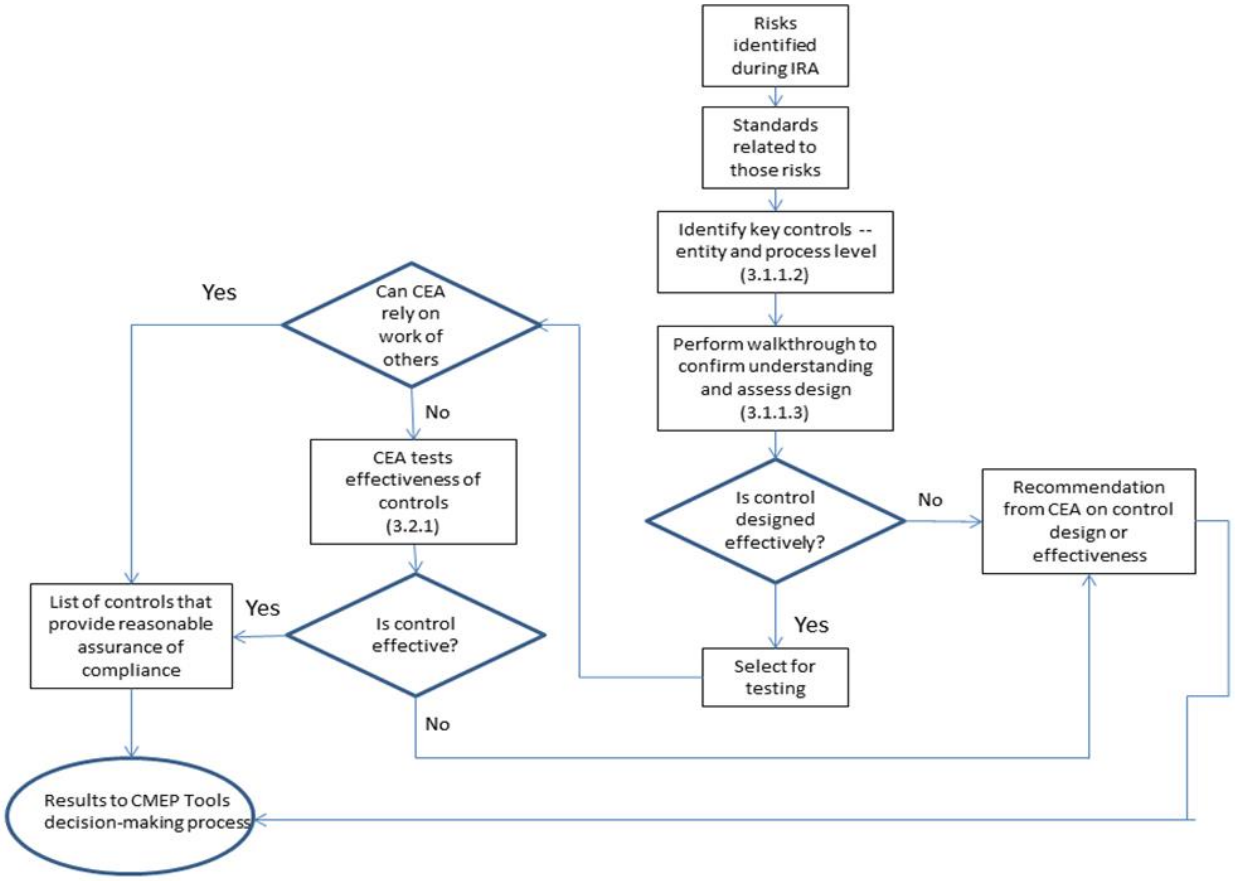


Figure 2: ICE Flow Chart

3.0 ICE Process

3. 1 Key Control Identification and Walkthrough

Guidance is provided for the following elements of this phase:

1. Key Control Identification
2. Walkthrough[4]/Control Design Analysis
3. Using the Work of Others

This section outlines how to identify key controls intended to mitigate or manage the subject risks and gather necessary information for inclusion in testing of internal controls. Once risks and associated standards and requirements are identified through the Risk Elements phase and analyzed during the Inherent Risk Assessment (IRA), the CEA will work with the registered entity to identify internal controls related to the entity's specific BPS risks and associated standards and requirements. The CEA will carefully tailor requests for information to the registered entity after reviewing applicable risks from the IRA and considering the information already available about the registered entity and its internal control environment. The CEA will then evaluate the design, implementation, and effectiveness of these controls.

Key Questions in Control Identification and Walkthrough Phase

3.1.1.2

- Has the entity established internal controls to address the standards and requirements associated with the IRA risk?
- What internal controls are most important to monitor to ensure applicable NERC Reliability Standard Compliance?

3.1.1.3

- When applied does the control produce the intended result?
- Is there sufficient, credible evidence to obtain reasonable assurance that the control produces the intended result?

3.1.1.4

- Does the entity monitor the control?
- Can the CEA use the results of the entity's monitoring to reduce compliance monitoring efforts?

3.1.1 Process

3.1.1.1. Key Inputs (Sources)

- Registered entity specific IRA report
- List of NERC Reliability Standards and Requirements to manage registered entity's risk to the reliability
- Past Audit Reports and Internal Control Evaluation results
- Compliance and self-report history
- Entity's culture of compliance[5]
- Information from neighboring organizations or operating agreements
- Third-party or independent evaluation reports previously provided by the registered entity[6]
- Entity information on internal controls associated with the results of IRA

[4] See Appendix A for a definition of the term "walkthrough."

[5] FERC has issued guidance on what makes an effective internal compliance program for registered entities. These factors shall be used by the CEA to understand the registered entity's culture of compliance. http://www.ferc.gov/whats-new/comm-meet/2008/101608/M-3.pdf

[6] Sources of other independent control evaluations may include: mock audits, applicable NRC reviews, other regional reviews, etc.

3.1.1.2 Identify Key Entity-level and Activity-level Internal Controls

In order to identify important or key internal controls (such as business processes, practices, policies, and procedures) to evaluate, the CEA must first understand how the registered entity's internal control program is designed to manage or 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 to support a conclusion that the internal control program or any portion of such program is effective.

The CEA will use the information resources above to identify key entity-level and activity-level internal controls.[7] Key controls and scoping of testing of key controls may be vetted in one or more of the following ways, which must be appropriately scaled and adapted to recognize the wide range of registered entity size, organizational structures, and risks to the BPS.

- Key internal controls might include those that represent the most likely point of failure regarding significant risks identified during the IRA. For example, if patch management was identified as a significant inherent risk for an entity, a failure point for this risk could be that the entity is not aware of the availability of a security patch, potentially leading to a subsequent failure to assess, test and install that security patch. A key internal control that a CEA may consider to prevent this failure is the implementation of an automated alert or notification system that advises entity's security personnel regarding the availability of a security patch, reducing the likelihood of a failure 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 in 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, et al) 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 to ignore 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 associated with a work-force preparedness risk. Conversely, in a large organization, a single type of power plant may be susceptible to an identified risk. It makes sense to only test those affected plants for internal controls associated with a particular risk, as the entire organization may not need a single internal control 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, and known control failures. The following table shows how some internal controls may be selected as key. This table does not include the rationale regarding all "non-key" internal controls and why they were not selected as key. Reasonable people might reach different conclusions on

[7] See Appendix A for a definition of entity-level and activity level controls.

which of internal controls are key and those that are not. The varying nature of risk and internal controls can lead two organizations to implement internal controls and monitoring procedures differently. Therefore, this example is not intended to represent a "best practice" for monitoring internal controls over the identified risks, or to imply that the non-key controls will never be monitored. Those responsible for monitoring controls in this risk area should be aware of how the internal control program addresses the risk and what controls provide the most support for their conclusions that the program is working. The table is not meant to imply a level of documentation, a preference of a particular automated or manual control, or a format that is necessary to support the identification of key internal controls. Rather, this table only illustrates several different internal control examples and how one internal control may be selected over another for evaluations purposes. Items marked with a 🔑 in this example are key internal controls selected for testing.

Risk Factor	Entity Provided Internal Control(s)	Key?	Rationale
Workforce Preparedness (CIP-004-3a,PER-003-1, PER-004-2,PER-005-2, PRC-001-1.1)	Management philosophy and communication in support of the corporate training program	🔑	This tone-from-the top internal control was selected as key because the risk is primarily one of integrity. If employees believe that training doesn't really matter to upper level management, they may be more likely to forego training activities. Conversely, if employees believe that it is not only against regulatory practice and company policy, but also against management's expressed desires, then the risk of an unprepared workforce may be reduced.
	Employees are manually reminded by their supervisor that they should complete their training 90 days prior to the due date of their NERC Reliability Standard Training		This may be an important internal control, but the effective operation of the next automated internal control described below will identify issues of non-compliance and correct it quickly. It is not necessary to test both of these important internal controls, as the automated internal control will illustrate the intended outcome. (Please note: If this internal control were present without the automated control, it may be selected for testing at the discretion of the CEA)
	When employees do not complete required training by the expected due date, their network access is disabled.	🔑	This is an automated internal control that would require employees to remain current on their training or lose their ability to perform their work. This internal control would mitigate the risk that employees are not properly prepared or trained for their duties[8].
Adverse Reliability impacts due to improper maintenance activities (PRC-005, PRC-008, TOP-001, FAC-003-	Management communicates and models the importance of proper system maintenance to staff and has a specific department dedicated to ensuring proper reliability system	🔑	This tone-from-the top internal control was selected as key because the risk is primarily one of integrity. If employees believe that maintenance doesn't really matter to upper level management, they may be more likely to forego training activities. Conversely, if employees believe that a deficiency in reliability system maintenance is not only against regulatory practice and company policy, but also against management's expressed desires, then the risk of not conducting system

[8] This is meant to illustrate an example of an automated control to ensure training. Such an automated control may not be practical or appropriate in all environments.

Risk Factor	Entity Provided Internal Control(s)	Key?	Rationale
3, PRC-004, PRC-006, PRC-021, PRC-022, EOP-005, EOP-004-2)	maintenance. This program includes communicating to appropriate authorities when systems do fail.		maintenance and not reporting errors to regulatory authorities will be reduced.
	Policies requiring proper system maintenance in accordance with NERC Reliability Standards		
	Standard maintenance cycles		This internal control is important, but changes in the standard maintenance cycles would be identified by the internal control set forth below.
	Management approval of deviation from standard maintenance cycle		Whenever a change in maintenance periods is input into the maintenance tracking system, management is notified and must approve the change in the cycle before field personnel will implement the change.
	Maintenance system policies state that any system event is properly researched and sent to appropriate authorities		This internal control is important, and may be identified as a key internal control at a smaller entity, in lieu of an automated internal control. However, if an automated escalation system is present (as in the control forth below), that internal control would be selected for testing during the ICE process
	Any outage on the system is automatically recorded and sent to management for review. The event must be responded to within 4 hours or it is escalated to the next level of management for review. Once a reportable event is recorded, internal audit is automatically notified to research the incident.		This is a key internal control, as it shows that events on the system will be identified and researched by appropriate levels of management. The automated, dual notification to the audit staff demonstrate that an independent party is also notified and will provide validation and follow up of the event.

3.1.1.3 Perform walk-through to confirm understanding of internal controls and assess design

Once the CEA has determined which internal controls to test, the CEA should perform a walkthrough to better understand the internal controls and ensure an appropriate internal control design. When evaluating the design of an internal control, the CEA needs to ensure that the information presented to validate the internal control is credible and sufficient.[9]

[9] For more information about sufficient appropriate evidence, please refer to the GAGAS Yellow Book, paragraphs 6.56 – 6.68 http://www.gao.gov/assets/590/587281.pdf

3.1.1.3.1 Information Credibility

Credible information gives the CEA reasonable (not necessarily absolute) assurance that the internal control program is effective for a given risk area and is relevant, reliable, and timely. After identifying which key internal controls are most appropriate for testing, the CEAs should inventory registered entity's internal control information to identify: (1) the current internal control information on file, (2) any outdated internal control information, and (3) any incomplete/missing internal control information.

3.1.1.3.2 Information sufficiency/amount of direct or indirect information to use in monitoring

The CEA should balance the use of direct and indirect information necessary to reach a conclusion that an internal control provides reasonable assurance to identify, manage or mitigate an identified risk. The CEA should confirm information collected is both appropriate and sufficient.

Appropriateness is a measure of the quality of information that encompasses its relevance, validity, and reliability, whereas sufficiency is a measure of the quantity of information that is necessary to draw conclusions. The following factors may be considered when reviewing the sufficiency of information about an internal control's operation: potential impact of an internal control's failure; whether an internal control operates in areas of great change in people, processes, or technology; how frequently an internal control operates, who is conducting the monitoring; corroboration provided by monitoring other internal controls; complexity of internal controls; the size of an entity; the level of significant judgment employed to conduct the internal control; whether an internal control is subject to management override; and whether the internal control is automated or manual in nature.

> Smaller entities will ordinarily have more informal internal controls that are carried out by one or a few persons. CEAs may rely on more observation and interviews to validate controls in these instances.

Risk Factor	Key Internal Control	Assess Information	Evidence to Support Conclusion
Workforce Preparedness (CIP-004-3a,PER-003-1, PER-004-2,PER-005-2, PRC-001-1.1)	Management philosophy and communication in support of the corporate training program	Sufficiency: Several sources (internal and external to the organization) validated management's philosophy and culture Credibility: Who has verified management's participation?	• Management participation and periodic compliance communications, meetings, including setting expectations that specifically address this risk and others • Meeting minutes validating Board level discussion of training violations
	When employees do not complete required training by the expected due date, their network access is disabled.	Sufficiency: Automated internal control – may be a sample of one observed action Credibility: Does automated system always work? Can anyone validate this is used? Who?	• Observation of automated process • Employee interviews confirming knowledge and effectiveness of the internal control

Risk Factor	Key Internal Control	Assess Information	Evidence to Support Conclusion
Critical systems become unavailable due to improper maintenance activities (PRC-005, PRC-008, TOP-001, FAC-003-3, PRC-004, PRC-006, PRC-021, PRC-022, EOP-005, EOP-004-2)	Management communicates importance of proper system maintenance to staff and has a specific department dedicated to ensuring proper reliability system maintenance. This program includes communicating when systems do fail to appropriate authorities.	Credibility: Validate communication during a recent outage, validate communication during any corrective action Sufficiency: Validation by more than one independent source	• Management participation in proper system maintenance training or communications • Corrective action as a result of failure to conduct system maintenance • Management review to verify that testing and maintenance was done using the established process.
	Management approval of deviation from standard maintenance cycle	Credibility: Validate that any changes to the maintenance cycle are approved by management by observation or automated logs Sufficiency: Validation by more than one source that this control works appropriately. Review logs from more than one recorded outage	• Observe automated process and obtained management approval of deviation.
	Any outage on the system is automatically recorded and sent to management for review. The event must be responded to within 4 hours or it is escalated to the next level of management for review. Once a reportable event is recorded, internal audit is automatically notified to research the incident.	Credibility: Validate that any outage is automatically recorded by checking logs or observing automated process Sufficiency: Validation by more than one independent source that this internal control works appropriately. Review logs from more than one recorded outage.	• Observe automated process • Obtain validation that event is responded to by management • Obtain response from internal audit

3.1.1.4 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.[10] An independent internal control evaluation may be conducted by a specialist, 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 by 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" based on any of these scenarios, the CEA team may review the independence, capabilities and competencies of the individuals performing the review and relevant Independent Audit Report (IAR) documentation for consideration of use as part of ICE evaluation. The information regarding a registered entity's independent review shall be gathered during the Key Control Identification and Walkthrough stage. Any additional information requests necessary will be sent to the registered entity, as necessary.

3.1.2 Outcomes

- List of Key Internal Controls selected for testing or reliance on the "work of others"
- Analysis of information to determine if the available information is relevant, reliable, timely, and sufficient
- List of information still needed to conduct an adequate evaluation of internal controls.
- Information request

3.2 Testing Effectiveness of the Internal Control Program (ICP)

Guidance is provided for the following elements of this phase:

1. Categorize Individual Controls
2. Assess Overall Internal Control Program

Key Questions for Testing Effectiveness of ICP Phase

3.2.1.2

- What types of internal controls has the entity identified in the ICP?
- Is there a blend of preventative, detective, and corrective controls to address each risk?

3.2.1.3

- Is the ICP implemented as designed?
- Is the ICP applied consistently?
- Is the intended risk effectively mitigated with the ICP?
- Does the entity identify, assess, and correct deficiencies in NERC Reliability Standards and Requirements?

With the prioritized risks identified via the IRA, the key internal controls selected (Section 3.1.1.2), and the available credible information identified (Section 3.1.1.3), the CEA has information available to make decisions about the effectiveness of the entity's internal controls[11], and, more importantly, whether the internal controls provide reasonable assurance of compliance with the identified NERC Reliability Standards. An effective program has individual internal controls that prevent, detect, or correct non-compliance with Reliability Standards. Though individual internal controls may fail, a well-designed internal control program can sustain failures and continue to operate effectively by properly aligning preventative, detective, and corrective controls and promoting a culture of compliance.

[10] CEAs shall recognize that Registered Entities may create internal control programs that aim to increase operational and compliance efficiencies. A registered entity shall not be punished for creating internal controls just for compliance nor be excluded from internal control evaluations for programs that are not created just for compliance.

[11] The complexity of an entity's internal controls may be commensurate with its size and risk to the BPS.

3.2.1. Process

3.2.1.1 Key Inputs (Sources)

- List of Key Internal Controls selected for testing or reliance on the "work of others" (See Section 3.1)
- Analysis of information to determine whether the information is relevant, reliable, timely, and sufficient
- List of information still needed to conduct an adequate evaluation of internal controls.
- Entity response to Section 3.1 information requests

3.2.1.2 Identify Categories of Internal Controls

When testing the effectiveness of internal controls, the CEA may recognize several categories of internal controls within an internal control program. The *RAI Internal Controls Working Guide*, July 09, 2013[12] identifies the following categories of internal controls:

Internal Control activities may be preventive, detective, and/or corrective. Examples are provided below:

- **Preventive Internal Control:** A preventive internal control is designed to discourage noncompliance with the Reliability Standards. They are proactive internal controls that help ensure the management objective of compliance with Reliability Standards. An example is a documented process that requires a training schedule be developed and maintained that includes all required training and the scheduling of training to ensure it is completed prior to the dates required by the applicable Reliability Standard requirements. This may be implemented by assigning training classes in a training tracking tool that notifies the individual of scheduled training, reminds individuals to complete the training, and notifies management that training has not taken place prior to the training deadline so management can take appropriate action.

- **Detective Internal Control:** A detective internal control is designed to find errors or irregularities and support effective compliance. An example is a documented process that requires a periodic review conducted to identify required training that was not completed as scheduled and training that was not completed per the Reliability Standard requirements. An example would be a quarterly review of completed training records to identify individuals that have not completed training by the required deadline.

- **Corrective Internal Control:** A corrective internal control is designed to assess instances of noncompliance and return an activity to a state of compliance. An example of a corrective internal control is automation of an Automatic Voltage Regulator (AVR) status indication so that an alarm occurs in the Transmission Operator's Control Center indicating an AVR status change from Automatic to Manual of a particular generating unit, thus providing notification to the TOP of an AVR status change within 30 minutes as required by Reliability Standard VAR-002.

[12] The Internal Control Working Guide was created, in partnership with Registered Entities, Regional Entities and various other stakeholders to help define and further the understanding of internal control programs and activities: http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/RAI%20Internal%20Controls%20Working%20Guide%20Document.pdf. That document provides useful information about internal controls but does not affect or supersede the process outlined in this Guide.

A smaller entity may address risks through one common internal control program, or through a combination of policies and procedures. A larger entity may devise their internal control program such that different internal control programs address different risks in different ways. The size and complexity of an internal control program shall effectively align with the size and complexity of the registered entity.

Because any internal control may fail, and a "perfect" internal control program is not possible, the CEA must use criteria for acceptable internal controls that provide reasonable assurance that the entity would be able to identify, assess, and correct errors in their environment in a timely manner. Thus, the purpose of identifying categories of internal controls is to recognize that an entity may have more than one method of identifying, assessing, and correcting reliability and/or compliance risk associated with the NERC standards and requirements. In some cases, a CEA may determine that one particularly strong internal control provides reasonable assurance of compliance, whereas in another case, a CEA may determine that a blend of preventative, detective, and corrective internal controls are necessary to provide reasonable assurance of compliance. The next section describes how a CEA may evaluate how effectively a risk is mitigated with a blend of internal controls or internal control program.

3.2.1.3 Assess Overall Internal Control Design

The CEA will utilize criteria for acceptable internal controls that provide reasonable assurance that the entity would be able to identify, assess, and correct errors in their environment in a timely manner. The criteria below aids in evaluating a level of implementation of a registered entity's internal controls.

Level of Internal Control Implementation	Meaning			
Label	**General Definition**	**Self-Monitoring (Preventative)**	**Promptness (Detective)**	**Anticipation (Corrective)**
Managed Internal Controls that are internally tested and Fully Implemented (FI)	Sufficient evidence and/or affirmations are present and judged to be adequate to demonstrate process and internal control implementation, and no significant weaknesses (relative to IRA-identified risk) are noted.	Multiple self-monitoring internal controls, most of which cannot be overridden without management notification/resolving issue	Detective internal controls that mitigate the risk factors within an acceptable time window	Combination of applicable corrective action plans or compensatory internal controls dealing with internal control failure and/or catastrophic risk impact. Other unexpected events are dealt with through well-defined and established procedures
Defined and documented Internal Controls that are Largely Implemented (LI)	Sufficient evidence and/or affirmations are present and judged to be	Some self-monitoring internal controls, at least one of which cannot be overridden without management	Majority of detective internal controls mitigate the	Variety of applicable corrective action plans or compensatory internal controls

Level of Internal Control Implementation	Meaning			
Label	**General Definition**	**Self-Monitoring (Preventative)**	**Promptness (Detective)**	**Anticipation (Corrective)**
	adequate to demonstrate process and internal control implementation, and one or more weaknesses are noted.	notification/resolving issue	risk factors and react fast enough to fix associated mishap well within an acceptable time window	dealing with internal control failure and/or catastrophic risk impact. Other unexpected events are dealt with through documented procedure
Repeatable Internal Controls or Partially Implemented (PI)	Data supplied to the team (evidence and/or affirmations) conflict –some data indicate the process and internal controls are implemented and some data indicate the practice is not implemented, and one or more significant weaknesses (relative to IRA-identified risk) are noted.	Some self-monitoring internal controls, which may include internal controls that cannot be overridden without management notification/resolving issue	Mixture of detective internal controls that at most times may mitigate the risk factors within an acceptable time frame.	At least one internal control that has a strong response/corrective action plan or compensatory internal control corrective action plan or compensatory control dealing with catastrophic impact of risk. Other unexpected events are dealt with through an informal procedures
Internal Controls Not Implemented (NI)	Some or all data required are absent or judged to be inadequate, data supplied does not support the conclusion that the process is implemented, and one or more significant weaknesses (relative to IRA-identified risk) are noted.	Some self-monitoring internal controls, most of which can be overridden without management notification/resolving issue	Some internal controls mitigate the risk, but not within an acceptable time window	Internal control may have a response/corrective action plan or compensatory internal control. Other unexpected events are dealt with intermittently through ad hoc procedures.
Internal Control is Missing (M)	The basic unit or support function has not yet reached the stage in the	No self-monitoring internal controls	No detective internal controls	No corrective action or compensatory internal control to deal with any issues

Level of Internal Control Implementation	Meaning			
Label	**General Definition**	**Self-Monitoring (Preventative)**	**Promptness (Detective)**	**Anticipation (Corrective)**
	sequence of work, or point in time to have implemented the process.			of internal control failure[13]

Note concerning application of internal control implementation criteria: The above-specified criteria shall be applied with careful consideration of an entities' size and risk profile. Internal controls shall always be commensurate with an entity's size and risk to the BPS. Smaller entities can qualify as having fully implemented internal controls without adopting unreasonable and unduly burdensome business processes or automated procedures. A CEA may determine that a smaller entity is able to achieve fully implemented internal control status through simple, yet well managed and supported, manual internal controls (e.g., relevant policies and procedures, with compliance confirmed through a management report and supported by a culture of compliance emanating from an internal compliance program).

The CEA will proceed through each risk item identified during the IRA and provide an evaluation for the internal control program(s) that addresses one or more of the risks identified in Risk Elements and vetted during the entity's IRA. Once completed with this process, the CEA will have an understanding of the internal control program strengths, weaknesses, and deficiencies by which to consider impact to the entity's compliance oversight plan.

3.2.2 Outcomes

- Assessment of the effectiveness of an entity's internal controls to address the risk factors
- Internal Control Program deficiencies
- Internal Control Program strengths and areas of improvement based upon implementation criteria

[13] Adopted from the Carnegie Mellon Capability Maturity Model Integration (CMMI®). http://whatis.cmmiinstitute.com/about-cmmi-institute

3.3 Finalize ICE Conclusions

The oversight of a particular entity is initially determined based on an inherent risk assessment. The lack of an ICE or the determination that the internal controls are inadequate will simply result in that regulatory oversight not being further tailored as a result of the ICE.
However, in formulating its oversight plan of a particular registered entity, the CEA may prioritize areas associated with identified control deficiencies as noted below.

Key Questions for Finalizing ICE Conclusions

- Do the internal controls mitigate the risks identified in the IRA?
- Where the internal controls do not completely mitigate the risk, should correction of the internal controls be encouraged, rather than focus on individual NERC Reliability Standard testing?
- How does the entity's internal controls inform the compliance oversight plan for this registered entity?

3.3.1 Process

The CEA shall prioritize control deficiencies using the following factors:

1. The likelihood that the deficiency will result in a violation of a NERC Reliability Standard. A deficiency means that there is some likelihood that a NERC Reliability Standard could be violated and 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, when monitored, can provide support for reducing the severity of a deficiency and the associated monitoring of relevant NERC Reliability Standards.
3. The potential effect of a control deficiency on the internal control program. An identified deficiency may be unimportant in relation to the overall working of the internal control program and management of risk, but it also may cause inefficiencies that cause greater risk to successful NERC Reliability Standard compliance
4. The aggregating effect of multiple deficiencies on NERC Reliability Standard compliance.

As the CEA prioritizes risk areas associated with any individual internal control deficiencies, focus must be kept on tailoring the compliance oversight plan for the registered entity. A deficient internal control does not mean a NERC Reliability Standard violation. A mildly deficient internal control may still result in modified (indirect) compliance oversight by the CEA. The CEA shall prioritize the residual risks based upon the entity's internal controls. The CEA will adjust the compliance oversight plan to examine NERC Reliability Standards not protected by an internal control.

3.3.2 Outcomes

- List of assessed internal controls that provide reasonable assurance of BPS reliability
- Revised draft compliance oversight plan for the registered entity based on internal control evaluation

The outcomes of ICE will be used by the regional entities to select appropriate CMEP Tools. The CEA will then finalize the custom compliance oversight plan for the registered entity.

3.4 Revision of the Internal Control Evaluation

The CEAs can review and revise the ICE of a registered entity at any time and should be cognizant of the effect that a registered entity's risks may pose to the reliability of the BPS. This understanding is essential in

performing ICE activities as it establishes a frame of reference by which the ICE is conducted. It is important to note that an ICE will need to be revised as new, emerging, or unique information is obtained and/or upon significant changes to the registered entity. For example, if an organization merges with another organization, and new individuals will be responsible for control implementation, the internal control may be tested again.

4.0 Documentation

4.1 Results Documentation

The CEAs should follow established Regional Entity documentation protocols, refer to the NERC Rules of Procedure, and use its professional judgment, where appropriate, when determining documentation needs throughout the ICE process. The extent of the resulting documentation is directly linked: (1) the nature, size, and complexity of the internal controls and review process, (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.

In any case, the CEA shall maintain documentation that clearly demonstrates their ICE and conclusions. Documentation includes all data and information obtained, reviewed, and used as inputs to the ICE.

4.2 Documentation Retention

Upon completion of the ICE process, the CEA will retain all relevant documentation that supports the procedures performed and conclusions reached. The CEAs should maintain all completed documentation, demonstrating the nature and extent of information reviewed and ICE conclusions reached. Documentation that should be retained includes, but may not be limited to, the following: ICE programs, 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 ICE process are also considered important documentation and should be retained.

When making the determination of the nature and extent of documentation that should be retained, the CEA should consider the information that would be required for an experienced compliance team member to understand the work performed and the conclusions reached during ICE activities. CEAs should maintain supporting documentation for review by NERC in connection with NERC's oversight of the compliance assurance program.

As NERC identifies improvements and best practices, it will provide additional guidance and training to CEAs.

5.0 References

Below are a list of reference materials that support the basic principles, concepts, and approaches within this Guide. The CEAs can use these reference materials to assist in applying the ICE process detailed in this Guide. These reference materials can assist with determining: (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.

- Generally Accepted Government Auditing Standards (GAGAS): http://gao.gov/assets/590/587281.pdf
- ERO Compliance Auditor Handbook: http://www.nerc.com/pa/comp/Pages/ERO-Enterprise-Compliance-Auditor-Manual.aspx
- Annual ERO CMEP Implementation Plan: http://www.nerc.com/pa/comp/Resources/Pages/default.aspx
- NERC Rules of Procedure (ROP): http://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx
- NERC Internal Control Working Guide: http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/RAI%20Internal%20Controls%20Working%20Guide%20Document.pdf

Appendix A – Definitions

Activity Level Internal Control Activity level internal controls are specific to a process or a function. These internal controls are designed to ensure the activity required by one or more Standards or requirements is completed as expected and either prevents or detects when the expected activity fails to be completed. An activity level internal control may address multiple functions across an entity but is not global in nature. Activity-level internal controls may be either manual or automated and include approvals, reviews, analysis, alarms, alerts, or systems.

Compliance Oversight Plan: The compliance oversight plan consists of the oversight strategy for a registered entity. The plan will usually include areas of focus, level of efforts, timing, and overall strategy on use of CMEP tool(s).

CMEP Tools: In context of IRA, CMEP tools are tools used during the compliance monitoring processes to develop the CEAs' Compliance Oversight Plan. CMEP tools are described in Section 3.0 of the NERC Rules of Procedure, Appendix 4C, and includes but are not necessarily limited to Compliance Audits, Spot Checks, Self-Certifications, and Periodic Data Submittals.

Detective Internal Control A detective internal control is an internal control designed to identify errors or deviations from the norm.

Entity Level Internal Control Entity level internal controls are pervasive across an organization. They include the 'tone from the top' including the organization's culture, values and ethics, governance, transparency and accountability mechanisms as well as the activities and tools put in place across the organization to raise staff awareness, ensure clear understanding of roles and responsibilities and solid capacities and abilities in managing risks well.

Inherent Risk Assessment: A review of potential risks posed by an individual registered entity to the reliability of the Bulk Power System (BPS).

Internal Control: Internal Controls are the processes, practices, policies or procedures an entity employs to comply with Reliability Standards that address risks associated with the reliable operation of its business. Examples may include: oversight, risk assessment, control activities, communications and training and monitoring. Internal Controls operate at both an entity or organizational level, as well as an activity or process level.

Internal Control Program: An Internal Control Program (ICP) is the set of Internal Controls an entity employs to comply with Reliability Standards and/or to address risks related to the reliable operations of the entity's business that were identified during the IRA. An Internal Control Program contains multiple Internal Controls that work together to produce compliant and reliable business operations.

Preventative Internal Control: A Preventative Internal Control is an Internal Control designed to avoid an unintended event or consequence

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).

Scope: The scope is the set of NERC Standards and Requirements to be reviewed in a given compliance oversight plan

Walkthrough/Walk-through: A walkthrough or walk-through is a procedure used during an evaluation of an entity's internal control to gauge the reliability of an internal control. A walk-though traces a process step-by-step from its inception to the final disposition.