Internal Controls Evaluation Report

Entity Name (ACRO)
NERC ID# NCR####

ICE Lead: RAM Member Name
Report Date: Month, DD, YYYY

Confidential Information – Do Not Distribute
# Table of Contents

- Executive Summary .......................................................................................................................... 2
- Purpose .............................................................................................................................................. 3
- Internal Controls Evaluation Process .................................................................................................. 3
- Assessment of the ACRO Internal Controls Program .......................................................................... 5
  - Evaluator Observations and Considerations for Improvement ........................................................... 6
- Assessment of ACRO’s Requirement-Level Internal Controls .............................................................. 7
  - STD-XX-XXX RXX ............................................................................................................................. 7
  - Design and Implementation Assessment ............................................................................................ 7
  - Evaluator Observations and Considerations for Improvement ........................................................... 8
  - Recommendation for COP Update ..................................................................................................... 8
- Document Information ......................................................................................................................... 8
- Appendix A ........................................................................................................................................ 9

# Executive Summary

The WECC conducted an Internal Control Evaluation (ICE) for Entity Name (ACRO) in YYYY. This report is a summary of WECC’s evaluation of ACRO’s internal controls.

WECC focused the scope of ACRO’s YYYY ICE on a subset of requirements chosen for audit in ACRO’s YYYY COP. WECC reviewed controls related to the following risk areas named in the COP during the YYYY evaluation:

**Example Scope**

- Program and Entity-Level Controls
- Requirement-Level Controls
  - Cyber Security — Configuration Change Management and Vulnerability Assessments (STD-XX-XXX RXX)
  - Cyber Security — Information Protection (STD-XX-XXX RXX)
  - Operating Personnel Communications Protocols (STD-XX-XXX RXX)
  - Transmission Vegetation Management (STD-XX-XXX RXX)
  - Facilities Ratings (STD-XX-XXX RXX)
  - Protection System Misoperation Identification and Correction (STD-XX-XXX RXX)
In this section, WECC will describe the scope of the ICE Evaluation and provide a high-level summary of the ICE assessment results.

WECC will consider results of the ICE to inform the risk-based approach in the development of future Compliance Oversight Plans (COP).

**Purpose**

As described in the ERO Enterprise Guide for Risk-based Compliance Monitoring\(^1\), and the ERO Enterprise Guide for Internal Controls\(^2\), WECC conducts ICE to refine the Registered Entity’s COP. The results of the ICE assessment do not change any obligation for the entity to comply with applicable NERC Reliability Standards. While the ICE process informs the COP, the ICE should not be seen as a limitation of WECC’s authority under the NERC Rules of Procedure to conduct any compliance monitoring activities as WECC may determine appropriate.

Given the many factors involved in designing and applying an effective internal control program, and the limited scope of controls assessed during ICE, the ICE evaluation does not guarantee an entity will never have a future incident of noncompliance with NERC’s Reliability Standards.

**Internal Controls Evaluation Process**

In this section, WECC will describe the process steps and timelines associated with the ICE.

This ICE report has, “considerations for improvement,” in which ICE has named practices that ACRO may wish to use to develop its internal controls. These considerations are not compliance findings and ACRO may use its discretion whether to apply the practices.

The ICE has two parts:

1. An evaluation of internal controls program maturity, and
2. The effectiveness of requirement-level controls related to the Standards in the scope of ICE.

The evaluation component objectives are described below:

**Internal Control Program Evaluation**

WECC assesses an entity’s internal controls program to see how the entity has developed and managed components that can consolidate processes, verify full implementation, design effective controls, and evaluate residual risk. The program-level evaluation focuses on the maturity of the program in the following areas: Risk Assessment, Design and Implementation, Monitoring, and Evaluation.

---

\(^1\) ERO Enterprise Guide for Compliance Monitoring, October 2016

\(^2\) ERO Enterprise Guide for Internal Controls, Version 2, September 2017
• **Risk Assessment** — WECC assesses how the entity detects risks related to the organization’s business and governance goals. Specifically, ICE looks at the entity’s “first line of defense,” or requirement-level risk assessment, and how the entity uses the assessment results to develop control goals that sufficiently cover the risks, or “failure points,” related to the entity’s business and governance goals. The goal of risk assessment is to identify a reasonable variety of potential failures.

• **Design and Implementation** — WECC looks at the processes the entity must develop and identify internal controls that respond to its business and governance objectives and that mitigate the related risks. ICE assesses the processes for how the entity ensures that current practices match documented controls as the entity’s policy, process, and procedure documents define them. ICE reviews the entity’s internal controls documentation to see the level of detail the entity has used to define its internal controls, such as:
  - Description of controls,
  - Source documents that reference the control,
  - Risks mitigated,
  - Frequency of operation,
  - Responsible personnel, and
  - Control classification (such as corrective, detective, or preventative; and key or non-key).

• **Monitoring** — WECC assesses the entity’s processes for internal review and testing internal controls in operation. WECC also assesses how the entity determines whether the controls are applied and working, and whether the entity understands their inherent and residual risks. WECC recommends timing and placement of monitoring that create opportunity to detect and correct issues prior to controls failures.

• **Evaluation** — WECC assesses the entity’s processes to consider feedback on control design and ensure that controls continue to meet risk objectives.

**Requirement-Level Controls Evaluation**

WECC assesses the requirement-level controls in two areas: control design and implementation. These areas are measured based on a qualitative and quantitative scale that reduces the discretion of the analyst.

• **Control Design** — WECC assesses the design of the internal controls as either *effective* or *deficient*. An effective control is one that meets the following requirements:

---

3 Failure points are risks found by the entity or WECC that can lead to noncompliance with Reliability Standards and Requirements, which can lead to potential risks to the BPS.

"Potential“ failure points give direction to registered entities as they assess risk while designing internal controls. The registered entity may use this document as a starting point in determining risk.
o Controls are designed to meet risk objectives (e.g., potential failure points.)
 o Control activities are documented in formal process and procedure documents to promote consistent performance of control activities.
 o The entity has internal controls documentation that describes control activities and enables the entity to monitor and evaluate internal controls.

- **Control Implementation**—WECC assesses whether the internal controls are operating correctly. Implementation is assessed with a rating of implemented, partially implemented, or not implemented. An implemented control is one that meets the following requirements:
   o Controls are in place and effectively mitigate risks.
   o The entity’s control activities and processes cover all known risks.

**Assessment of the ACRO Internal Controls Program**

An effective system of internal control reduces, to an acceptable level, the risk of not achieving an entity objective and may relate to one, two, or all three categories of objectives. It requires that:

- Each of the four components and relevant principles are present and functioning. “Present” refers to the determination that the components and relevant principles exist in the design and implementation of the system of internal control to achieve specified objectives.
  
  “Functioning” refers to the determination that the components and relevant principles continue to exist in the operations and conduct of the system of internal control to achieve specified objectives.

The program components operate together in an integrated manner. “Operating together” refers to the determination that all components collectively reduce, to an acceptable level, the risk of not achieving an objective. Components should not be considered discretely; instead, they operate together as an integrated system. Components are interdependent with a multitude of interrelationships and linkages among them, particularly the manner in which principles interact within and across components.

**Premise of the Evaluation:**

- Design of “controls” are geared to achieve a stated objective(s). In reference to the NERC Reliability Standards, two objectives are essential: compliance and operations.
  
  o **Compliance objective:** Controls are designed and implemented to support entities’ compliance (reporting) obligations.
  
  o **Operations objective:** Controls are designed and implemented to achieve the reliability and security objectives of the requirement(s).

- Controls compositions consisting of ongoing tasks and activities (outline of the means to an end)

- Controls factored people and the actions they take at every level of an organization to affect internal control
Controls Design and Implementation components, assumed operating with zero error, are able to provide reasonable assurance.

Controls adaptability/applicability within the entity structure—(flexible in application for the entire entity or for a particular subsidiary, division, operating unit, or business process)

Evaluator Observations and Considerations for Improvement

In this section, WECC will describe how the entity’s internal control program addresses each evaluation area, as defined above.

Overall Internal Controls Program Assessment: **Level #: Level Name**

- Level 1: Informal or ad-hoc
- Level 2: Standard
- Level 3: Managed and Monitored
- Level 4: Optimized

Risk Assessment

- Notes of the evaluator’s observation of the entity’s internal control program component of Risk Assessment.
  - Consideration – Evaluator recommendation(s) of opportunities for entity internal controls program improvement in the area of Risk Assessment.

Design and Implementation

- Notes of the evaluator’s observation of the entity’s internal control program component of Design and Implementation.
  - Consideration – Evaluator recommendation(s) of opportunities for entity internal controls program improvement in the area of Design and Implementation.

Monitoring

- Notes of the evaluator’s observation of the entity’s internal control program component of Monitoring.
  - Consideration – Evaluator recommendation(s) of opportunities for entity internal controls program improvement in the area of Monitoring.

Evaluation

- Notes of the evaluator’s observation of the entity’s internal control program component of Evaluation.

---

4 See Appendix A
Consideration – Evaluator recommendation(s) of opportunities for entity internal controls program improvement in the area of Evaluation.

Recommendation for COP Updates

In this section, WECC will describe any impacts to the entity’s COP based on the maturity of the internal controls program.

Assessment of ACRO’s Requirement-Level Internal Controls

The following section outlines WECC’s assessment of ACRO controls related to specific NERC Reliability Standards in scope of ICE. This summary is not a complete list of controls reviewed by WECC, but a highlight of WECC’s observations and assessments of the control’s implementation.

The following table is a summary of ICE results for ACRO.

<table>
<thead>
<tr>
<th>Standard and Requirement</th>
<th>Control Design</th>
<th>Control Implementation</th>
<th>Recommended COP Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>STD-XX-XXX RXX</td>
<td>Effective or Deficient</td>
<td>implemented, partially implemented, or not implemented</td>
<td>Impact to COP</td>
</tr>
<tr>
<td>STD-XX-XXX RXX</td>
<td>Effective or Deficient</td>
<td>implemented, partially implemented, or not implemented</td>
<td>Impact to COP</td>
</tr>
<tr>
<td>STD-XX-XXX RXX</td>
<td>Effective or Deficient</td>
<td>implemented, partially implemented, or not implemented</td>
<td>Impact to COP</td>
</tr>
<tr>
<td>STD-XX-XXX RXX</td>
<td>Effective or Deficient</td>
<td>implemented, partially implemented, or not implemented</td>
<td>Impact to COP</td>
</tr>
</tbody>
</table>

STD-XX-XXX RXX

Design and Implementation Assessment

Control Design: Effective or Deficient

Control Implementation: implemented, partially implemented, or not implemented
Evaluator Observations and Considerations for Improvement

In this section, WECC will describe how the entity’s internal controls address the potential failure points defined by WECC.

Potential Failure Point: Failure to...

- Observation #1
- Observation #2
- Observation #3
  - Consideration – Evaluator recommendation(s) of opportunities for entity internal controls program to improve risk mitigation in this area.

Potential Failure Point: Failure to...

- Observation #1
- Observation #2
- Observation #3
  - Consideration – Evaluator recommendation(s) of opportunities for entity internal controls program to improve risk mitigation in this area.

Recommendation for COP Update

In this section, WECC will describe any impacts to the COP based on the entity’s internal controls specific to the standard.

Document Information

<table>
<thead>
<tr>
<th>Document Approval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
</tr>
<tr>
<td>-------</td>
</tr>
</tbody>
</table>
Appendix A

<table>
<thead>
<tr>
<th>Requirement-Level Controls</th>
<th>Internal Controls Program</th>
<th>Program Maturity</th>
</tr>
</thead>
</table>
| The entity has requirement-level controls that marginally mitigate reliability risk. | The entity has insufficient program-level components that do not effectively identify activity and process level risk, provide controls design and implementation governance, monitor controls performance, address controls efficacy, repeatability, and sustainability. | **Level 1: Informal or ad-hoc**  
- No formal controls framework exists to define key requirement objectives  
- Insufficient risk identification  
- Fragmented/unstructured control activities  
- Lack of control consistency across various lines of business, “silo” situations  
- Control activities dependent upon tribal knowledge and/or individual heroics  
- Unstructured/informal documentation and reporting methods  
- Unstructured/informal monitoring methods  
- Unstructured/informal documentation and reporting functions  
- Control may be designed and implemented but no assurance they remain current |
<table>
<thead>
<tr>
<th>Requirement-Level Controls</th>
<th>Internal Controls Program</th>
<th>Program Maturity</th>
</tr>
</thead>
<tbody>
<tr>
<td>The entity has requirement-level controls that mitigate reliability risk.</td>
<td>The entity has program-level components that generally identify reliability risk, provide controls design and implementation governance, monitor controls performance, address controls efficacy, repeatability, and sustainability.</td>
<td><strong>Level 2: Standard</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A semi-formal controls framework exists to define key requirements and objectives</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• General identification of reliability risk</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Activity and process level controls generally mitigate reliability risk</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Limited program governance and program components may exist, but not implemented across multiple lines of business</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Limited accountability and performance monitoring of controls performance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Limited control alignment/structure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Limited implementation consistency across various lines of business, little to no “silos” situations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Limited control activities dependent upon tribal knowledge or individual heroics</td>
</tr>
<tr>
<td>Requirement-Level Controls</td>
<td>Internal Controls Program</td>
<td>Program Maturity</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| The entity has requirement-level controls that distinctively mitigate activity and process level reliability risk. | The entity has program-level components that adequately identify activity and process level risk of reliability, provide controls design and implementation governance, monitor controls performance, address controls efficacy, repeatability, and sustainability. | **Level 3: Managed and Monitored**

- A formal controls framework exists to define key requirements and objectives
- Effective activity and process level risk identification
- Activity and process level controls adequately mitigate reliability risk
- Program governance and program components exist, implemented across multiple lines of business
- Managed accountability and performance monitoring of controls performance
- Control alignment/structure
- Control implementation consistency across various lines of business, no “silo” situations
- Limited to no control activities dependent upon tribal knowledge or individual heroics |
<table>
<thead>
<tr>
<th>Requirement-Level Controls</th>
<th>Internal Controls Program</th>
<th>Program Maturity</th>
</tr>
</thead>
</table>
| The entity has requirement-level controls that optimally mitigate reliability risk. | The entity has solid program-level controls that adequately identify activity and process level risk of reliability, provide controls design and implementation governance, monitor controls performance, address controls efficacy, repeatability, and sustainability. | **Level 4: Optimized**

- A well implemented formal controls framework exists to define key requirements objectives
- Operations-governed activity and process level risk identification
- Activity and process level controls fully mitigate reliability risk
- Formalized, structured program components implemented across multiple lines of business
- Managed accountability and real-time or near real-time performance monitoring of controls
- Control alignment/structure
- Control implementation consistency across various lines of business, no “silo” situations
- Limited to no control activities dependent upon tribal knowledge or individual heroics
- Benchmarking, best practices and continuous improvement measures are incorporated into program operation
- Key Performance Indicators (KPI) are defined for monitoring effectiveness |