MARCH 21, 2023

RELIABILITY & SECURITY

Virtual Workshop

WECC

Supply Chain Risk Management

March 21, 2023

Stacia Carron

Teri Kelly

Morgan King

Tom Williams

Objectives

- Learn how multiple NERC Standards holistically address risks to the supply chain and mitigate procurement risks
- Learn how program maturity can lead to a differentiated approach to audit

Main Messages

- Risk-based CMEP means differentiated experiences
- Investments in compliance culture matter
- Example: Just because two entities have CIP-013 in scope does not mean we would take the same approach to auditing them
- Depending on an entity's program, history, and controls, approach to audit and gaining assurance can be different

Supply Chain Compliance Requirements

A mature and effective program to mitigate risks associated with supply chain will consider related NERC Standards holistically

- CIP-013-2
- CIP-010-4 (R1.6)
- CIP-005-7 (R2.4, R2.5, R3)

Differentiated Approach to Audit

- A differentiated approach to audit is based on entity-specific risk and control objectives
- These objectives will influence how auditors make determinations of reasonable assurance
- For example, CIP-013 is scoped for both Orko and Sunbear Power, but these entities have different risk and control objectives and so our approach to auditing CIP-013 would be different

Going into the Audit

	Orko	Sunbear Power
Audit Scope	CIP-013-2 (R1), CIP-010-4 (R1.6), and CIP-005-7 (R2.4, R2.5, R3)	
Compliance Program	Historically has demonstrated strong compliance program. WECC risk objectives are, therefore, limited and targeted to specific processes. Orko communications with WECC are collaborative and transparent.	Challenged compliance history. Little is known about Sunbear's compliance program; therefore, WECC risk objectives are at Standard or program level. Sunbear communications with WECC are rare and minimal.
Controls	Provided detailed controls in ICDCT response.	Provided minimal ICDCT response (just a list of documents without providing the documents). Documentation lacked details and did not identify controls.
Data Provided	Comprehensive RSAW. Complete ERT L1 response. ERT Level 2 responses provided evidence needed to assess compliance to requirements.	RSAW provided little information other than listing document names. ERT L1 response was complete. ERT Level 2 responses lacked evidence requested to assess compliance to requirements.

Audit Experience

	Orko	Sunbear Power
Auditors' knowledge of Supply Chain Program	The auditors were well informed on Orko's CIP-013 program ahead of audit.	Since auditors have little or no knowledge of Sunbear's CIP-013 program or controls, the audit experience was more complicated.
Auditors Request of Entity	The auditors issued only one Request for Information and held one interview. The audit closed three days early.	The auditors submitted 10 Requests for Information and held three interviews just for CIP-013.
Controls Assessment	Most of the interview was devoted to a demonstration by Orko of its CIP-013 controls and plans to improve those controls over the next three years.	The controls assessment required more time and Requests for Information.
Outcome	Risk team later determined lower monitoring priority for CIP-013.	The auditors found one Potential Noncompliance and four Areas of Concern and a higher monitoring priority for CIP-013.

Audit Compliance Findings

Orko

Potential Noncompliance
- OEA: Self-Report for not updating its Supply Chain Risk Management plan to include procurement of PACS and EACMS associated with BES Cyber Systems

Positive Observations
- Applying its plan to the procurement of low impact BES Cyber Systems
- An exceptionally detailed plan that includes internal controls
- Including contract renewals in its plan

Recommendations
- Implement controls to verify CIP-013 R1.2.5 methods are defined for a vendor before authorizing changes that deviate for the existing baseline configuration
- Implement controls to verify CIP-013 R1.2.3 processes are in place before granting vendor access

Sunbear Power

Potential Noncompliance
- Not updating its Supply Chain Risk Management plan to include procurement of PACS and EACMS associated with BES Cyber Systems

Areas of Concern
- Not describing in its plan how identified risks are assessed and handled
- Not including in its plan open-source software, freeware, and other services procured without exchange of funds
- Not including procurements from a vendor contracted before October 1, 2020
- Performing risk assessments on resellers on but not on OEMs (Original Equipment Manufacturers)

Recommendation
- Establish an internal controls program to implement detective and preventive controls

Auditor Notes to Risk and Controls Teams

	Orko	Sunbear Power
Controls Assessment	Comprehensive and detailed supply chain program including good preventive and detective controls to mitigate procurement risks to the BES.	Weak supply chain program and lack of controls introduce procurement risks to the BES.
Notes to Risk Team	**CIP-013-2 R2** Self-Certification with Evidence to validate implementation of planned controls. **CIP-005-7 R2.4, R2.5, and R3** Check in with Orko ahead of the next audit to see whether anything has changed with vendor remote access and connections. **CIP-010-4 R1.6** Check in with Orko ahead of the next audit on their project to improve controls for verifying software source and identity.	**CIP-013-2** The audit team recommends scoping both R1 and R2 at the next audit. **CIP-005-7 R2** The audit team recommends scoping all of R2 at the next audit. **CIP-010-4 R1** The audit team recommends scoping all of R1 at the next audit to assess configuration change management process in addition to verification of software source identity.

Key Takeaways

The factors we consider to gain reasonable assurance of compliance could change depending on the strength of an entity's controls

- Scopes will map to specific risks and control objectives
- Similarly scoped entities could have different experiences at audit depending on their compliance history controls maturity
- Auditor observations are inputs to the Compliance Oversight Plan

Key Takeaways

- The investment that an entity makes in developing a good program can directly affect the approach to the audit
- An entity that shows strong compliance history and controls will afford greater assurances that factor into future engagements
- If auditors are unable to glean information on controls from the submitted evidence, there could be more Requests for Information and interviews

WECC

Electric Reliability and Security for the West

www.wecc.org