Electric Reliability and Security for the West

Controls Guidance and Compliance Failure Points

CIP-013-2

Entity Coordination
Identity Management and Access Control

November 2022

WECC Intent

The *Controls Guidance and Compliance Failure Points* document guides registered entities in assessing risks associated with their business activities and designing appropriate internal controls in response. WECC's intent is to provide examples supporting the efforts of registered entities to design controls specific to operational risk *and* compliance with the NERC Reliability Standards. The registered entity may use this document as a starting point in assessing risk and designing appropriate internal controls. Each registered entity should perform a risk assessment to identify its entity-specific risks and design appropriate internal controls to mitigate those risks; WECC does not intend for this document to establish a standard or baseline for entity risk assessment or controls objectives.

> ***Note:*** *Guidance questions help an entity understand and document controls. Any responses, including lack of affirmative feedback, will have no consequences on an entity's demonstration of compliance during a Compliance Monitoring and Enforcement Program (CMEP) engagement.*
>
> ** Please send feedback to internalcontrols@WECC.org with suggestions on controls guidance and potential failure points questions.*

Definitions and Instructions

Control Objective: Aim or purpose of internal control to address identified risk or operational concern.

Control Activities: Policies, procedures, techniques, and mechanisms to achieve control objectives and mitigate related risks.

Quality Assurance/Quality Control (QA/QC): How an entity *verifies* it performed an activity or verifies an activity was performed *correctly* (examples include separation of duties, having a supervisor double-check someone's work, *etc*.).

Risk Category: Type of operational and inherent risks identified by the ERO Enterprise for use in the Compliance Oversight Plan (COP). Entities should use Risk Categories to understand, monitor, and mitigate known and future risks.

Risk Category

Entity Coordination: Coordination among entities, both internally and externally, as well as third-party

suppliers and contractors, is necessary before making changes to the system or taking any actions that have the potential to impact another entity and, in turn, may impact the reliability and security of the Bulk Power System (BPS). Coordination should address the risk associated with operating horizon, planning horizons, and during emergencies. Failure to coordinate may result in an impact on the reliability and security of the BPS.

CIP-013-2 specifically requires risk mitigation with respect to incident coordination, vendor access management, vulnerability monitoring, and verification of vendor software and patches. Failure to coordinate both internally and externally in any of these instances could jeopardize the BPS through to successful malicious activity.

Identity Management and Access Control: Entities must develop controls to prevent or mitigate malicious or unintentional access to BES Cyber Assets. Failure to develop controls may compromise the integrity and operability of the BPS. The three major tenets of security controls are to provide confidentiality, integrity, and availability (CIA).

CIP-013-2 requires an entity to work with its suppliers to prevent malicious or unintentional access that takes advantage of vulnerabilities inherent in vendor products, services, or processes.

Control Objective(s)

Your entity should perform a risk assessment and identify entity-specific control objectives to mitigate those risks. To help your entity get started, WECC has identified generic control objectives to mitigate the risks associated with the risk categories mentioned above and CIP-013-2. You may want to consider these three objectives:

> **Control Objective 1:** Ensure cyber security risks associated with your entity's suppliers and associated products and services are identified. (Relates to Entity Coordination)
>
> **Control Objective 2**: Ensure processes are in place to mitigate identified cyber security risks. (Relates to Identity Management and Access Control)
>
> **Control Objective 3**: Ensure vendors abide by agreements to mitigate cyber security risks. (Relates to Entity Coordination)
>
> **Control Objective 4**: Coordinate supply chain risk management activities across internal processes. (Relates to Entity Coordination)

Reliability and Security Control Activities

Control activities are how your entity meets your control objectives. As you design controls, your entity should tailor them to entity-specific control objectives.

Below are examples of control activities based on good practices WECC has observed that are designed to

meet the objectives listed above. WECC does not intend for these activities or the associated questions to be prescriptive. Rather, they should help your entity consider how you might meet your objectives in your own unique environment. They also may help your entity identify controls you did not realize you had.

Control Objective 1: Ensure cyber security risks associated with your entity's suppliers and associated products and services are identified.

Control Activity A: Implement a process to identify and assess cyber supply chain risk (Relates to risk associated with R1.1)

1. How does your entity identify and assess cyber supply chain risk?
    a. What standards, frameworks, and methods do you use to identify and assess risk?
    b. How do you record and communicate risk assessment findings or updates?
    c. How do you involve internal stakeholders in risk assessments?
    d. How do you coordinate among different departments or business units when required?
    e. How do you use your internal expertise to develop and assess risk for supply chain management?
    f. How do you ensure that your operational subject matter experts have the training and skills needed to carry out the supply chain risk management plan?
2. How does your entity determine if a risk is acceptable?
    a. Do you have guidelines for the determination of acceptable risk?
    b. Who has the authority to make that determination?
    c. Are there any reviews of that determination?
3. Does your process use any third-party assessments or certifications? If so,
    a. How does the third-party risk identification feed into your risk assessment process?
    b. How do you ensure the third-party risk assessment aligns with your organizational plan to assess identified risk?
4. How does your entity analyze supply chain cyber security risk of procurements made under existing contracts?
    a. Does your plan address software license renewals, maintenance agreements, etc.?
    b. If so, how do these topics feed into your risk assessment process?
5. How does your entity assess risk of emergency purchases?
    a. Do you have an alternate risk assessment process?
    b. Have you clearly defined what situations qualify for this process?
    c. Who is allowed to authorize the use of this process?

Control Activity B: Assess vendor-specific risks. (Relates to risk associated with R1.1)

1. What criteria does your entity consider when assessing vendor-specific risks? (e.g., data security, geography)
2. How does your entity evaluate the vendor's relationship with your business and operational needs?

(e.g., product, service, or both; manufacturer, reseller, or turnkey provider)
3. How does your entity evaluate the risk associated with the vendor's suppliers? (e.g., third-party software installed on vendor's hardware)
4. How does your entity ensure risks specific to transitioning from one vendor to another are evaluated for relevant procurements?
5. What are the roles and responsibilities of the BES Cyber System owners in the evaluation?
6. How does your entity update, communicate, and document vendor-specific risks?

Control Activity C: Assess product or service-specific risks (Relates to risk associated with R1.1)

1. What criteria does your entity consider when assessing product-specific risks? (e.g., manufacturing limitations, sourcing restrictions, repair history, etc.)
2. What process does your entity use to assess open-source software?
    a. Do you utilize third-party sources for assessments and reports of applicable open-source software incidents or vulnerabilities?
3. What process does your entity use to assess contracting or temporary employee providers?
4. What are the roles and responsibilities of the BES Cyber System owners in the evaluation?
5. How does your entity update, communicate, and document product or service-specific risks?

Control Activity D: Monitor and update risk assessments if needed.

1. How does your entity monitor for changes to risks?
    a. Do you periodically survey vendors to determine if risks have changed?
    b. Do you use third parties to monitor for emerging threats?
2. How does your entity manage renewal agreements or service subscriptions?
    a. Do renewal agreements require updated risk assessments?
    b. Do service subscriptions require periodic risk assessments?
    c. How do you ensure processes are in place to mitigate cyber security risks that are identified after contracts are already in place?
3. How does your entity evaluate supply chain risk outside of the procurement cycle?
    a. What events trigger risk assessment updates? (e.g., vendor mergers and acquisitions, vendor contracts with new suppliers, product end of life)
    b. Do you perform re-evaluations on a specific timetable? (e.g., yearly)
    c. Do you use any automated tools to track periodic risk reviews?

Control Objective 2: Ensure processes are in place to mitigate identified cyber security risks.

Control Activity A: Develop standard protocols to mitigate vendor risks. (Relates to risk associated with R1.1)

1. How are standard mitigating measures determined?
2. How does your entity communicate your organizational risk criteria to vendors?

a. Defined requirements
b. Request for proposals
c. Bid evaluations

Control Activity B: Mitigate identified cyber security risks that are not covered by standard contractual terms. (Relates to risk associated with R1.1)

1. How are mitigating controls negotiated with vendors when standard contractual terms are not sufficient? (i.e., customized contractual terms)
2. How are mitigation methods determined for risks the vendor does not agree to mitigate?
3. How does your entity ensure all identified risks have associated mitigating measures?

Control Activity C: Define plan for vendor incident coordination (Relates to risk associated with R1.2.1 and R1.2.2)

1. How does your entity define and communicate to vendors what constitutes a qualifying vendor incident and requires notification?
2. What methods does your entity use to receive vendor incident notifications?
3. How does your entity ensure notifications are communicated to the personnel responsible to act?
    a. Are there escalation paths and intervals in place to ensure prompt responses to vendor identified incidents?
    b. Do you maintain specific guidance for activating your cybersecurity incident response plan?
    c. How will you manage vendor-identified incidents that do not trigger your cybersecurity incident response plan?
    d. How will you assess and record vendor-identified incidents for future cyber supply chain risk considerations?

Control Activity D: Define and apply vendor access protocols (Relates to risk associated with R1.2.3 and R1.2.6)

1. What technical and procedural controls does your entity have in place to track and manage vendor remote or on-site access?
2. What technical and procedural controls does your entity have in place to disable active vendor remote access if needed?
3. How does your entity require vendors to notify you when remote or onsite access should be removed?
4. What controls are in place to respond to these notifications and timely revoke remote or on-site vendor access?
5. Does your entity perform any QA/QC to ensure (1) All provisioned vendor access has a business need and (2) remote or on-site revocations are prompt?

Control Activity E: Define or apply vulnerability disclosure protocols. (Relates to risk associated with

R1.2.4)

1. How has your entity defined what constitutes a "known vulnerability"?
2. How are requirements for vendors to report required disclosures documented?
    a. Do you define methods for reporting?
    b. Do you define a timeframe for reporting?
3. How will your entity assess and record vendor vulnerabilities for future cyber supply chain risk considerations?

Control Activity F: Define software integrity and authenticity verification processes. (Relates to risk associated with R1.2.5)

1. What methods does your entity use to verify the integrity and authenticity of the software or patches obtained from vendors?
    a. Are these methods defined contractually?
2. How does your entity manage and record exceptions when there is no method to verify the integrity and authenticity of the software obtained from the vendor?
    a. Are additional control measures in place for these exceptions?

Control Objective 3: Ensure vendor abides by agreements to mitigate cyber security risks.

Control Activity A: Monitor vendor performance.

1. What controls are in place to ensure post-sale communication with vendors?
2. How does your entity hold vendors accountable for taking agreed-upon actions to mitigate cyber security risks?
    a. Does your standard contract include incentives or penalties?
3. How does your entity verify vendors are meeting contractual obligations?
    a. Does your standard contract establish periodic reviews?
    b. Do you use any automated tools to track periodic reviews of vendor performance?

Control Activity B: Ensure vendor cyber security risks are mitigated.

1. How does your entity implement additional mitigating activities where vendors are not meeting contractual obligations to mitigate cyber security risk?

Control Objective 4: Coordinate supply chain risk management activities across internal processes.

Control Activity A: Ensure supply chain risk assessments are triggered from appropriate internal processes.

1. How does your entity ensure assets are properly classified and identified as applicable?
    a. Is supply chain risk management integrated into your change management process?
    b. When existing assets are re-classified (and become applicable), is the supply chain risk

assessment process triggered?

c. When new assets are commissioned, is the supply chain risk assessment performed prior to acquiring assets that are not yet classified?

2. How does your entity ensure procurements made during response and recovery from cybersecurity incidents follow the Supply Chain Risk Management Plan?
3. How does your entity ensure applicable purchases cannot be made with procurement cards without appropriate risk assessment?

Control Activity B: Ensure supply chain risk management activities are coordinated with internal processes.

1. How has your entity implemented processes to mitigate vendor-identified vulnerabilities?
   a. Does the vendor vulnerability disclosure process integrate into the software patching process?
   b. Does the vendor vulnerability disclosure process integrate into the cyber security incident identification process?
2. Do your entity's internal processes include a mechanism for identified risks or vulnerabilities to be considered in future vendor or product risk assessments?
   a. Are vulnerabilities discovered during CIP-010 vulnerability assessments fed into future risk assessments?
   b. Are vulnerabilities discovered during Cyber Security Incident response or recovery activities fed into future risk assessments?
   c. Does the identification of vulnerabilities trigger an update to an existing risk assessment?

Compliance Potential Failure Points

The control activities listed above are specifically targeted at mitigating risk to the reliability and security of the BPS, but also promote compliance with the referenced standard. Your entity should also develop controls specifically to mitigate compliance risk. The following compliance potential failure points relate directly to compliance risk and warrant consideration.

Potential Failure Point (R1): Failure to document supply chain risk management plan(s) that addresses all the elements in Requirement 1.

1. Does your entity perform any QA/QC to confirm all elements of the requirement are addressed in the documented plan(s)

Potential Failure Point (R2): Failure to implement supply chain risk assessment processes, policies, and strategies.

1. What controls does your entity have in place to document and verify the application of the plan to the procurement process?

2. How does your entity ensure the plan is applied and managed consistently across the organization?

Potential Failure Point (R3): Failure to review and approve the plan at least once every 15 calendar months.

1. How does your entity track timeframes for review and approvals?
    a. Do you use alarms or alerts?
2. What review process does your entity have in place to assess whether the plan is effective?
    a. Do you update the risk assessments to address emerging supply-chain-related vulnerabilities?
    b. If so, do you consult guidance from outside sources such as NERC, E-ISAC, ICS-CERT, and CCIRC?
3. What process does your entity have in place to update the plan if the review indicates changes are required?
4. How are changes to the plan communicated to the organization?
5. What QA/QC does your entity perform to verify the review and approval occur at least once every 15 calendar months?