WECC
Electric Reliability and Security for the West

Controls Guidance and Compliance Failure Points

CIP-008-6

Emergency Operations Planning
Operating During Emergencies/Backup & Recovery

October 2023

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 North American Electric Reliability Corporation (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: The aim or purpose of specified controls; control objectives address the risks related to achieving an entity's objectives.

Control Activities: The policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the entity's objectives and address related risks.

Internal Control: Internal controls are the processes, practices, policies or procedures, system applications and technology tools, and skilled human capital an entity employs to address risks associated with the reliable operation of its business. Internal control components include:

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring

Quality Assurance/Quality Control (QA/QC): How an entity *verifies* whether 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 Electric Reliability Organization (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

Emergency Operations Planning: Entities must have the necessary facilities, tools, processes, and procedures to prevent or respond to system events, emergencies, or unexpected conditions. Failure to develop adequate plans may result in gaps that could lead to a compromise of bulk power system (BPS) reliability and security.

Operating During Emergencies/Backup & Recovery: Entities must act during an emergency, system event, or unexpected conditions that could result in instability, uncontrolled separation, or cascading outages within an interconnection. This can include:

- Ensure personnel are sufficiently prepared and have adequate access to the procedures, processes, tools, and facilities to respond appropriately and effectively.
- Ensure adherence to processes and procedures.
- Ensure proper operation, availability, and use of facilities and tools.

Control Objectives

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 within CIP-008-6. You may want to consider these four objectives:

Control Objective 1: Ensure personnel recognize and properly evaluate a Cyber Security Incident.

Control Objective 2: Ensure an appropriate response to a Cyber Security Incident.

Control Objective 3: Appropriately communicate during and after a Cyber Security Incident.

Control Objective 4: Ensure the plan is effective.

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 unique environment. They also may help your entity identify controls you did not realize you had.

Control Objective 1: Ensure personnel recognize and properly evaluate a Cyber Security Incident.

Control Activity A: Develop, distribute, and maintain guidance for recognizing a Cyber Security Incident. (Relates to risk associated with R1)

1. Does your entity have a matrix, workflow, or similar document to identify benign/normal events against malicious/suspicious events?
   a. Does that document include realistic examples of threats to your system?
   b. How do you make that document available to personnel in an emergency?
2. Does your entity provide communications regarding security incident recognition and evaluation to the entire organization as part of security awareness?

Control Activity B: Train personnel to recognize a Cyber Security Incident. (Relates to risk associated with R1)

1. How does your entity identify personnel for training?
   a. How do you ensure personnel receive training to recognize a Cyber Security Incident?
   b. At what frequency do you conduct training?
2. How does your entity ensure your training is effective?
   a. Does your training include realistic scenarios?
   b. Is the training interactive?
   c. Do you update your training periodically to consider emerging risks?
   d. Does your training include scenarios where responsible personnel are not available (e.g., natural disaster)?

Control Activity C: Monitor systems to identify events. (Relates to risk associated with R1)

1. What monitoring systems does your entity have in place to quickly detect an attempt to compromise?
   a. How do you investigate events of interest (anomalies) to determine whether an attempt to compromise an applicable system occurred?
   b. Do you monitor for both physical and electronic attempts?
   c. Is monitoring technical (e.g., intrusion detection system) or manual (e.g., security guard)?
   d. Who receives the notification of potential attempts to compromise?
   e. How is that notification received? (e.g., push notification, audible alert)

Control Objective 2: Ensure an appropriate response to a Cyber Security Incident.

Control Activity A: Develop, distribute, and maintain guidance for handling a Cyber Security Incident. (Relates to risk associated with R1)

1. Does your entity have a matrix, workflow, or similar document to guide Cyber Security Incident response while responding?
    a. Does that document include realistic examples of threats to your system?
    b. Are these documents dynamic to allow for response to uncommon events?
    c. Do these documents account for events that occur after hours or during other downtimes?
    d. How do you make that document available to personnel in an emergency?
    e. How do you ensure that the document is the most current version?

Control Activity B: Train personnel in their roles and responsibilities. (Relates to risk associated with R1, R3)

1. How does your entity identify and document roles and responsibilities?
    a. How do you ensure personnel are aware of their roles and responsibilities? (e.g., read receipts, acceptance documents)
    b. How do you track changes to roles and responsibilities?
    c. Do you include alternate roles and responsibilities to ensure bench strength during an event?
    d. Do personnel understand how roles and responsibilities might differ when personnel are unavailable (e.g., during a natural disaster)?
2. Does your entity perform any additional response training outside of the Cyber Security Incident response plan test?
    a. Do you participate in any industry group drills? (e.g., GridEx)
    b. Do you provide any role-based security incident training specific to responders?
    c. Do you perform exercises during non-working hours or weekends?

Control Objective 3: Appropriately communicate during and after a Cyber Security Incident.

Control Activity A: Ensure sufficient information is communicated externally.

1. What external entities does your entity coordinate with both during and after an incident?
    a. Interconnected entities?
    b. Local law enforcement or emergency services?
    c. State or federal law enforcement or emergency services?
    d. Public relations?
    e. ERO Enterprise, NERC, and the Federal Energy Regulatory Commission (FERC)?
2. Does your entity have a checklist or job aid to ensure the appropriate information is communicated to each external entity?

Control Activity B: Report Cyber Security Incidents to appropriate authorities. (Relates to risk associated with R4)

1. Does your entity have a process to investigate suspicious or anomalous activity to determine whether an incident is reportable or non-reportable?
    a. Have you defined criteria used to determine reporting obligations?

2. How does your entity ensure you notify appropriate agencies within the specified time frame?
    a. Which entities are you required to report Cyber Security Incidents to?
    b. Which additional external entities do you report Cyber Security Incidents to?
3. How does your entity define responsible personnel to make incident notifications?
    a. Do you have personnel on call to aid in the notification during an emergency?
4. What attributes does your entity report to external entities?
    a. Do you communicate all 10 National Cybersecurity and Communications Integration Center (NCCIC) requested attributes to all external entities?
    b. Do you have any other information that you communicate to external entities?

Control Activity C: Coordinate with vendors. (Relates to risk associated with R1)

1. When a vendor notifies your entity of an incident related to their product or services, how is that evaluated to determine whether a response is necessary?
2. What mechanisms does your organization have to communicate with vendors during an incident?
    a. How do you determine whether you need additional vendor support (e.g., technical support) during an incident?
    b. Who is responsible for that coordination?
3. How does your entity ensure vendors are aware of vulnerabilities in their product that may have been discovered during an incident?
    a. Do you report incidents involving vendor products even if the product vulnerability/cause of the incident is not clear?

Control Activity D: Communicate with relevant internal personnel.

1. During an incident, how does your entity communicate with other parts of the organization that may be affected by the incident either directly or indirectly?
    a. What type of technical support is available outside of the affected organization?
2. How does your entity structure the transition to recovery plans including preservation of data during the incident as appropriate?
3. How does your entity communicate the outcome of security event investigations and Cyber Security Incident response plan tests to responders and the organization as a whole?

Control Objective 4: Ensure the plan is effective.

Control Activity A: Ensure Cyber Security Incident response plan is designed to mitigate likely threats.

1. Does your entity monitor for emerging cybersecurity threats?
2. Does your entity work with peer organizations to share threat information, review incident response methods and tools, and collaborate on robust, real-life Cyber Security Incident response plan testing scenarios?
3. Has your entity participated in any outside assessments to determine likely threat vectors? (e.g., the Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Evaluation Tool (CSET))

   a. If so, how do you update and reinforce guidance for responders based on these insights?

Control Activity B: Coordinate incident response testing internally. (Relates to risk associated with R2)

1. Does your entity coordinate testing between multiple departments, facilities, or impact levels?
   a. Do you maintain multiple related plans?
   b. If so, how do you ensure they work together?
2. When using a regional or national exercise (e.g., GridEx) to complete the 15-month exercise of the Cyber Security Incident response plan, how does your entity ensure the Cyber Security Incident response plan was incorporated into the exercise?
   a. How is that documented?
3. How does your entity select exercise scenarios for the Cyber Security Incident response plan test?
   a. Do you include both cyber- and physical scenarios during test exercises?
   b. Do you select exercise scenarios that are applicable to low, medium, and high impact Bulk Electric System (BES) Cyber Systems?
   c. Do you combine CIP-009 with CIP-008 test exercises?
   d. How do you ensure robust real-life scenarios?
4. How does your entity ensure the necessary personnel are included in the Cyber Security Incident response plan test?
   a. Do you involve personnel from all parts of your organization (e.g., Information Technology (IT), Operational Technology (OT), compliance, corporate)?
5. How does your entity test detection tools during incident response tests?

Control Activity C: Incorporate lessons learned from a Cyber Security Incident or an incident response test. (Relates to risk associated with R3)

1. How does your entity identify lessons learned?
   a. Do you identify lessons learned as the incident or exercise unfolds?
      i. Do you have a dedicated scribe when the Cyber Security Incident response plan is activated?
   b. Do you conduct a post-incident meeting to identify lessons learned or the absence of lessons learned?
   c. Who participates in identifying lessons learned?
2. How does your entity ensure lessons learned are meaningful?
   a. What methods do you use to solicit ongoing feedback from responders?
   b. Do you solicit feedback regarding process improvements? resource constraints? operational efficiencies?
3. How does your entity ensure lessons learned are incorporated into the Cyber Security Incident response plan?

Control Activity D: Update the incident response plan to address system and organizational changes.

(Relates to risk associated with R3)

1. How are system or organizational changes identified?
    a. Is someone responsible for monitoring for changes that would affect the plan?
2. Who is responsible for updating the Cyber Security Incident response plan due to system or organizational changes?
3. Who is responsible for disseminating the updates to the Cyber Security Incident response plan?

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 Cyber Security Incident response plan(s) that include the applicable requirement parts.

1. Identify, classify, and respond to Cyber Security Incidents.
2. Criteria to evaluate and define attempts to compromise.
3. Process to determine if a Cyber Security Incident is a Reportable Cyber Security Incident or an attempt to compromise an applicable system.
4. A process to notify the Electricity Information Sharing and Analysis Center (E-ISAC) and the United States National Cybersecurity and Communications Integration Center (NCCIC) when a Reportable Cyber Security Incident or attempt to compromise an applicable system is identified.
5. Roles and responsibilities of Cyber Security Incident response groups or individuals.
6. Incident handling procedures for Cyber Security Incidents.

Potential Failure Point (R2, R3, R4): Failure to clearly define or communicate start and end dates used to establish time frames for reporting incidents or testing and updating the plan.

Potential Failure Point (R2): Failure to test each Cyber Security Incident response plan at least once every 15 calendar months.

Potential Failure Point (R2): Failure to use the Cyber Security Incident response plan when responding to or conducting an incident response plan exercise.

Potential Failure Point (R2): Failure to document deviations from the plan during the response to the incident or exercise.

1. Does your entity use a checklist or similar job aid to ensure deviations from the plan are identified, reviewed, and addressed?
2. How are personnel trained to recognize when a deviation exists?

Potential Failure Point (R2): Failure to retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise an applicable system.

1. What types of records are maintained?
2. Where are they maintained?
    a. Do you maintain a repository for all Cyber Security Incident response activities?
    b. Do you use any technology solutions to maintain documentation?
3. Who is responsible for retaining records?
4. Are records reviewed to verify accuracy and completeness?

Potential Failure Point (R3): Failure to notify those with a role in the Cyber Security Incident response plan when there are applicable changes to the plan.

1. How does your entity identify applicable changes?
2. How does your entity notify personnel of changes to the plan?
3. How does your entity ensure timelines are met?
4. How does your entity document notifications?
5. Does your entity document acceptances of these notifications?

Potential Failure Point (R3): Failure to document lessons learned or absence of lessons learned within 90 calendar days after completion of a Cyber Security Incident response plan test or actual Reportable Cyber Security Incident response.

Potential Failure Point (R3): Failure to update the Cyber Security Incident response plan based on documented lessons learned within 90 calendar days after completion of a Cyber Security Incident response plan test or actual Reportable Cyber Security Incident response.

1. Does your entity have any automated tools (e.g., workflow) used to ensure updates are made promptly?

Potential Failure Point (R3): Failure to notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned within 90 calendar days after completion of a Cyber Security Incident response plan test or actual Reportable Cyber Security Incident response.

1. How does your entity ensure personnel receive notifications? (e.g., email read receipts, acknowledgment form)

Potential Failure Point (R3): Failure to update the Cyber Security Incident response plan no later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the entity determines would affect the ability to execute the plan.

1. Does your entity have any automated tools (e.g., workflow) used to ensure updates are made promptly?

Potential Failure Point (R3): Failure to notify each person or group with a defined role in the Cyber Security Incident response plan of the updates within 60 calendar days after a change was made to the plan.

1. How does your entity ensure personnel receive notifications? (e.g., email read receipts, acknowledgment form)

Potential Failure Point (R4): Failure to provide E-ISAC or NCCIC with the minimum attributes:

1. Functional impact
2. Attack vector used
3. Level of intrusion that was achieved or attempted.

Potential Failure Point (R4): Failure to provide notification to E-ISAC and NCCIC within the required time frames.

Potential Failure Point (R4): Failure to provide updates to E-ISAC and NCCIC within the required time frames when the determination of new or changed attributes is known.