Electric Reliability and Security for the West

Controls Guidance and Compliance Failure Points

CIP-003-8

Emergency Operations Planning
Training
Asset/System Management and Maintenance
Asset/System Physical Protection

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.

Internal Control: The plans, methods, policies, and procedures to fulfill a mission, goals, and objectives. Internal control components include:

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

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

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 BPS reliability and security.

Training: Personnel/operators must have adequate knowledge and skills to ensure BPS reliability and security. Failure to adequately train personnel may compromise BPS reliability and security.

Asset/System Management and Maintenance: BPS reliability depends on an entity's success in tracking, managing, and maintaining significant amounts of data, components, assets, and systems. The scope and complexity of this effort require programs to ensure that the entity effectively performs these activities. Failure to execute these programs can result in various types of lapses and may compromise the integrity and reliability of the BPS.

Asset/System Physical Protection: Failure to physically protect BES assets could lead to access by unauthorized personnel leading to actions resulting in instability, uncontrolled separation, or cascading within an Interconnection.

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-003-8. You may want to consider these six objectives:

Control Objective 1: Ensure personnel understand the Cyber Security objectives of the organization. (Relates to Training)

Control Objective 2: Control physical access to low impact BES Cyber Systems and associated Cyber Assets. (Relates to Asset/System Physical Protection)

Control Objective 3: Control electronic access to low impact BES Cyber Systems and associated Cyber Assets. (Relates to Asset/System Management and Maintenance)

Control Objective 4: Ensure personnel are prepared to respond to a Cyber Security Incident. (Relates to Emergency Operations Planning, Training)

Control Objective 5: Ensure Cyber Security Incidents are reported to appropriate groups for further analysis. (Relates to Asset/System Management and Maintenance, Asset/System Physical Protection)

Control Objective 6: Protect BES Cyber Systems from the introduction of malicious code via Transient Cyber Assets or Removable Media. (Relates to Asset/System Management and Maintenance, Asset/System Physical Protection)

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 personnel understand the Cyber Security objectives of the organization.

Control Activity A: Implement the Cyber Security Policy(ies) in the organization. (Relates to risk associated with R1)

1. How does your entity ensure your Cyber Security Policy is followed?
2. How does your entity ensure relevant employees understand the Cyber Security Policy(ies)?
    a. Do you train employees on how the policy(ies) affect their work?
        i. How do you evaluate the effectiveness of the training provided?
        ii. Do you test your employees following training?
    b. How do you ensure changes to the policy(ies) are communicated to relevant personnel?

Control Activity B: Determine the target audience for cyber security awareness. (Relates to risk associated with Requirement R2, Attachment 1, Section 1)

1. How does your entity determine which personnel need to receive cyber security awareness training and communications?
    a. Do you include contractors or vendors?
2. How does your entity ensure personnel have received reinforcement of cyber security practices?
3. How does your entity ensure new hires are aware of cyber security practices?

Control Activity C: Distribute cyber security awareness material. (Relates to risk associated with Requirement R2, Attachment 1, Section 1)

1. How does your entity select cyber security awareness material?
    a. Who is responsible for selecting the material?
    b. Is this part of an enterprise-wide program or a separate targeted program?

   c. How do you verify the content is appropriate for your target audience?
   d. Do you differentiate your awareness material by job function/role?
   e. Do you include physical security practices that affect cyber security in your awareness materials?
2. How does your entity ensure receipt of cyber security awareness material?
   a. Who is responsible for distributing the material?
   b. What media do you use for distribution?
   c. How do you ensure receipt of the material?
3. How does your entity ensure timely distribution of cyber security awareness material?
   a. How frequently do you reinforce cyber security practices?

Control Objective 2: Control physical access to low impact BES Cyber Systems and associated Cyber Assets.

Control Activity A: Define methods of physical access control to protect assets with low impact BES Cyber Systems. (Relates to risk associated with Requirement R2, Attachment 1, Section 2)

1. How does your entity identify the locations that need physical security?
   a. Do you specify protection at an asset level or BES Cyber System level?
   b. What are your procedures to identify all low impact BES Cyber Assets that require physical security measures?
   c. How do you ensure Cyber Assets that provide electronic access controls are protected if they are not co-located with the BES Cyber System?
   d. How do you manage any changes to the assets or location of the low impact BES Cyber Systems?
   e. How do you know when low impact assets and Cyber Assets that provide electronic access are added or removed?
   f. What are your procedures to develop, review, update and approve diagrams?
   g. How do you address physical access control responsibilities at locations that are shared with other entities?
2. Does your entity conduct a risk assessment or threat evaluation to determine the points that are in most need of protection?
   a. If so, how is the risk assessment conducted?
   b. What risk elements are considered in the risk assessment? (e.g., asset criticality, threat actors, threat vectors, vulnerabilities, mitigating controls, physical topology, information about known breaches at similar BES Cyber Systems)
3. How does your entity identify methods of protection?
   a. Do you match methods of protection to identified threats?
   b. How do you document protection methods?
   c. How do you make employees aware of these methods?

4. How does your entity ensure physical access is limited to those with a need to access the asset or the location of the BES Cyber System?
    a. If you use hard keys, do you have a key control plan?
    b. What actions are taken if a key is lost?
    c. What are your processes to request, review and approve physical access?
    d. Do you periodically review physical access authorization records?
    e. Does your employee offboarding process include notifications of employee transfers and terminations to other business functions?
    f. How does your entity ensure that physical access authorizations are revoked promptly when no longer needed?
    g. Do you review and validate physical access authorizations after an Incident Response/Recovery (i.e., confirm all accounts were restored, confirm previously revoked accounts were not restored)?

Control Objective 3: Control electronic access to low impact BES Cyber Systems and associated Cyber Assets.

Control Activity A: Identify electronic communications to and from each asset containing low impact BES Cyber System(s) to determine which electronic communications are in scope. (Relates to risk associated with Requirement R2, Attachment 1, Section 3)

1. How does your entity confirm that you have identified all routable communications between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System?
    a. How do you determine whether the communication uses a routable protocol when entering or leaving the asset?
    b. How do you identify time-sensitive protection or control function communications between intelligent electronic devices?
2. How does your entity confirm that all relevant SMEs are involved in the identification process?
3. How does your entity ensure the use of accurate technical documents?
4. How does your entity monitor for changes to the BES Cyber System that would affect its electronic access controls? (e.g., additions, replacements)
    a. Do you employ asset inventory controls to detect discrepancies between cyber asset inventory lists and actual cyber asset inventory?
5. How does your entity review scoping determinations for completeness and correctness?

Control Activity B: Implement electronic access controls for each asset containing low impact BES Cyber System(s) (Relates to risk associated with Requirement R2, Attachment 1, Section 3)

1. How does your entity determine electronic access control methods?
    a. Is it based on a vulnerability or threat assessment?

   b. If so, how frequently are vulnerabilities reviewed?
2. How does your entity determine what inbound and outbound electronic access is ***necessary***?

3. What processes does your entity employ to approve, implement, and review electronic access controls?
4. How does your entity approve and implement, and review electronic access rules?
   a. Is the "deny all others by default" rule explicitly stated in the access control lists (ACLs) and firewall rules?
   b. How do you ensure your "deny all others by default" rule is not overridden by another policy (e.g., permit any/any)?
5. How does your entity ensure electronic access is limited to those with a need to access the asset or the location of the BES Cyber System?
   a. What processes does your entity have in place to grant, review, and revoke electronic access to low impact BES Cyber Systems?
   b. Do you document shared or generic account information with the names of individuals who have knowledge of them?
   c. Does your employee offboarding process include notifications of employee transfers and terminations to other business functions?
   d. In the event of transfers or terminations, does your entity change shared or generic account passwords?
   e. Do you review and validate electronic access authorizations after an Incident Response/Recovery (i.e., confirm all accounts were restored, confirm previously revoked accounts were not restored)?
6. Do you collect and review security logs related to access control (e.g., successful login attempts, failed login attempts, failed access attempts)?
7. How does your entity ensure that inbound and outbound permissions are not changed without proper justification and authorization?
8. Does your entity have methods to prevent and detect malicious communications?
9. How does your entity detect unauthorized changes to the electronic access of low impact BES Cyber Systems?

Control Activity C: Authenticate Dial-up Connectivity to low impact BES Cyber System(s). (Relates to risk associated with Requirement R2, Attachment 1, Section 3)

1. How does your entity ensure all devices with Dial-up Connectivity are identified?
2. How does your entity ensure the defined authentication method(s) address all assets using Dial-up Connectivity?
3. How does your entity document authentication methods?
4. How does your entity make employees aware of methods?

Control Objective 4: Ensure personnel are prepared to respond to a Cyber Security Incident.

Control Activity A: Ensure personnel are prepared to identify a Cyber Security Incident. (Relates to risk associated with Requirement R2, Attachment 1, Section 4)

1. How are personnel notified of suspicious or malicious activity?
2. What criteria does your entity use to determine if a security event is a Cyber Security Incident?
    a. What thresholds have been developed to delineate normal activity against suspicious activity?
    b. How do you classify events with an undetermined cause?
3. How does your entity verify all relevant personnel understand the criteria used to identify a Cyber Security Incident?
    a. Do you train all personnel to recognize a Cyber Security Incident?
    b. Do you conduct refresher training? If so, how often?
    c. Do you provide guidance documents that would be accessible during an event?
    d. How do you ensure that every employee has knowledge of the process and contact information to report suspected security incidents?

Control Activity B: Define roles and responsibilities for low impact BES Cyber System incident response plan(s). (Relates to risk associated with Requirement R2, Attachment 1, Section 4)

1. How does your entity determine roles and responsibilities for low impact BES Cyber Security Incident response plan(s)?
    a. Do you have alternate Cyber Security Incident response team members?
    b. Do you have any supplier agreements to provide support during security incidents?
2. How does your entity notify personnel they have a role/responsibility in the Cyber Security Incident response plan?
3. How does your entity verify all personnel with responsibilities in the incident response plan understand their role?
    a. Do you require individuals or groups to sign an acceptance of responsibilities document?
4. How does your entity track and update changes to roles and responsibilities?
5. Does your entity employ outside vendors to assist in incident response?

Control Activity C: Develop actionable incident handling procedures. (Relates to risk associated with Requirement R2, Attachment 1, Section 4)

1. How does your entity develop effective incident handling procedures?
    a. Do the procedures provide any decision matrix or process diagrams tools to assist in the response to security incidents??
    b. Do the procedures include clear instructions on when and how to escalate CSI responses and communicate with stakeholders?
    c. Do the procedures include information on how to coordinate response efforts with vendors

when appropriate?

2. How does your entity ensure any external references in the plan(s) (e.g., contact lists, checklists) are kept updated and accessible during an actual response or recovery?
3. How does your entity ensure employees understand these procedures?
    a. Do you train all personnel on incident handling procedures?
    b. Do you provide guidance documents (such as checklists or decision trees) for use during an event?

Control Activity D: Test Cyber Security Incident response plan(s). (Relates to risk associated with Requirement R2, Attachment 1, Section 4)

1. How does your entity ensure timely testing of incident response plans?
2. How does your entity ensure all relevant personnel are included in incident response plan testing?
    a. Who determines which personnel and business units should participate in response planning and testing?
    b. Do you perform personnel and site rotations to ensure that all process stakeholders from every site have the opportunity to participate in incident response exercises?
    c. What are your participant selection criteria?
3. How does your entity define and communicate testing methods or strategies to parties responsible for performing testing of incident response plans?
    a. How do business units coordinate testing efforts?
    b. How do you select realistic scenarios for testing?
    c. If your low impact Cyber Security Incident response plan is combined with high or medium impact Cyber Security Incident response plans, how do you ensure scenarios are relevant to low impact BES Cyber Systems?
    d. How do you ensure relevant incident handling methods are tested?
4. How does your entity verify incident response plant testing is effective?

Control Activity E: Update Cyber Security Incident response plan(s). (Relates to risk associated with Requirement R2, Attachment 1, Section 4)

1. How does your entity confirm relevant changes are made to Cyber Security Incident response plan(s)?
    a. Do you include lessons learned from (1) test(s) and (2) actual Reportable Cyber Security Incident(s) in plan changes?
    b. Do your controls include quality assurance to determine the efficacy of the new plan(s)?
2. How does your entity ensure that all incident response plan stakeholders are aware of any changes to Cyber Security Incident response plan(s)?

Control Objective 5: Ensure Cyber Security Incidents are reported to appropriate groups for further analysis.

Control Activity A: Develop criteria to determine reporting obligations. (Relates to risk associated with Requirement R2, Attachment 1, Section 4)

1. How does your entity evaluate potentially applicable legal and regulatory security incident reporting requirements?
2. How does your entity monitor for changes to legal and regulatory reporting requirements?

Control Activity B: Report Cyber Security Incidents to the appropriate agencies. (Relates to risk associated with Requirement R2, Attachment 1, Section 4)

1. How does your entity identify Reportable Cyber Security Incidents?
    a. Who is responsible for determining if a Cyber Security Incident is reportable?
2. How does your entity notify appropriate agencies including:
    a. Electricity Information Sharing and Analysis Center (E-ISAC)?
    b. Law enforcement?
    c. Other?
3. Does your entity identify a timeline for reporting Cyber Security Incidents in low impact BES Cyber Systems?

Control Objective 6: Protect BES Cyber Systems from the introduction of malicious code via Transient Cyber Assets or Removable Media.

Control Activity A: Mitigate the risks of malicious code introduction from entity-owned Transient Cyber Assets (Relates to risk associated with Requirement R2, Attachment 1, Section 5)

1. How does your entity manage entity-owned Transient Cyber Assets?
    a. Do you maintain an asset list of all entity-owned Transient Cyber Assets?
    b. If so, what information is documented for each asset?
2. What methods are used to detect malicious code on Transient Cyber Assets?
3. What methods are used to mitigate the risk of introduction of malicious code? (e.g., software or antivirus updates)
    a. Are these methods applied in an ongoing or on-demand manner?
    b. What automated or manual tools are in place to manage Transient Cyber Assets?
4. How does your entity confirm the proper mitigations have been completed before connecting the Transient Cyber Asset?
    a. How do you ensure all relevant personnel understand the mitigation methods for Transient Cyber Assets?
    b. What training is provided to personnel on the Transient Cyber Asset process?
5. What Quality Control methods does your entity have in place to ensure methods to mitigate the risk of introduction of malicious code are properly employed on all relevant entity-owned Transient

Cyber Assets?

6. What methods does your entity use to detect or prevent the connection of unauthorized Transient Cyber Assets?

Control Activity B: Mitigate the risks of malicious code introduction from Removable Media. (Relates to risk associated with Requirement R2, Attachment 1, Section 5)

1. How does your entity control the use of Removable Media?
    a. What methods are used to detect malicious code on Removable Media?
    b. What mitigation process is in place in the case of detecting malicious code on Removable Media?
    c. How do you confirm the proper mitigations have been completed before connecting the Removable Media?
    d. Do you employ measures to restrict unauthorized access to physical ports? If so, are they physical (e.g., physical port locks) or administrative (e.g., policies and procedures)?
    e. Do you deploy a centralized method, such as a USB hub to scan and transfer files into your networks?
2. How does your entity ensure all relevant personnel understand the mitigation methods for Removable Media?
    a. Do you have acceptable use policies that communicate standards of behavior concerning the proper use of entity-owned hardware?

Control Activity C: Ensure vendors mitigate the risk of malicious code from Transient Cyber Assets and Removable Media. (Relates to risk associated with Requirement R2, Attachment 1, Section 5)

1. How does your entity mitigate the risk of introduction of malicious code from Transient Cyber Assets that are managed by a third party?
    a. How do you communicate Transient Cyber Asset security requirements to third parties?
    b. How do you confirm the proper mitigations have been completed before connecting the Transient Cyber Asset?

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 develop a cyber security policy.

1. Does your entity have a review process that ensures all topics are collectively addressed?
2. How does your entity document your review activity?

3. How does your entity ensure your CIP Senior Manager approves the policies?
4. How does your entity document your approval activity?
5. How does your entity ensure review and approval activities are completed within the required period?

Potential Failure Point (R1, R2): Failure to develop a process for declaring and responding to CIP Exceptional Circumstances

1. Does your entity have policies and procedures for handling CIP Exceptional Circumstances?
    a. How do you define when a CIP Exceptional Circumstance should be declared?
    b. Who can declare a CIP Exceptional Circumstance?
    c. How do you ensure the process is not too cumbersome to follow during an emergency?
2. How does your entity ensure that all personnel understand what a CIP Exceptional Circumstance is and what appropriate responses are?

Potential Failure Point (R2): Failure to implement comprehensive cyber security plan(s) for assets containing low impact BES Cyber Systems.

1. Does your entity have a QA/QC process that ensures all topics are collectively addressed and up to date?
2. How does your entity document your review activity?
3. How does your entity ensure plan(s) are implemented and effective?

Potential Failure Point (Requirement R2, Attachment 1, Section 1): Failure to distribute relevant cyber security awareness material at least once every 15 calendar months.

1. How does your entity ensure it reinforces cyber security practices at least once every 15 calendar months?
2. Does your entity perform any QA/QC to verify cyber security awareness material is relevant and timely?

Potential Failure Point (Requirement R2, Attachment 1, Section 2): Failure to control physical access, based on need to assets or locations of low impact BES Cyber Systems and Cyber Assets that provide electronic access controls.

1. How does your entity document your methods to control physical access?
2. How does your entity determine and document the need for physical access?
3. How does your entity identify Cyber Assets that provide electronic access controls?
4. How does your entity ensure your physical access controls are working properly?

Potential Failure Point (Requirement R2, Attachment 1, Section 3): Failure to develop a policy requiring inbound and outbound access controls.

1. How does your entity document your policy for inbound and outbound access?

Potential Failure Point (Requirement R2, Attachment 1, Section 3): Failure to develop a process to understand inbound and outbound traffic.

1. How does your entity determine required controls for inbound and outbound communications?
2. How does your entity document the reasons for granting permissions for inbound and outbound access?

Potential Failure Point (Requirement R2, Attachment 1, Section 4): Failure to document one or more processes to identify, classify, and respond to Cyber Security Incidents.

1. Has your entity established criteria to determine whether a security event is a Cyber Security Incident?
2. Has your entity established criteria to classify Cyber Security Incidents?
3. How does your entity verify the criteria are complete?
4. Has your entity documented incident response processes?

Potential Failure Point (Requirement R2, Attachment 1, Section 4): Failure to identify the roles and responsibilities of personnel or groups within the Cyber Security Incident response team.

1. How does your entity document roles and responsibilities for low impact BES Cyber System incident response plan(s)?
    a. Are roles documented by individual or group?

Potential Failure Point (Requirement R2, Attachment 1, Section 4): Failure to document incident handing procedures for Cyber Security Incidents.

1. How does your entity document incident handling procedures (e.g., procedures, workflows, job aids)

Potential Failure Point (Requirement R2, Attachment 1, Section 4): Failure to use the Cyber Security Incident response plan when responding to a Cyber Security Incident or conducting an incident response plan exercise.

1. How does your entity ensure that all required tasks are followed when responding to Cyber Security Incidents (e.g., checklists)?

Potential Failure Point (Requirement R2, Attachment 1, Section 4): Failure to meet Cyber Security Incident response deadlines.

1. How does your entity ensure the Cyber Security Incident response plan is tested at least once every 36 calendar months?
    a. How do you track upcoming exercises?
    b. How do you notify personnel of upcoming exercises?
2. How does your entity ensure the Cyber Security Incident response plan is updated (if needed) within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or

actual Reportable Cyber Security Incident?

Potential Failure Point (Requirement R2, Attachment 1, Section 4): Failure to report a Reportable Cyber Security Incident to the E-ISAC.

1. Has your entity documented criteria to determine if a Cyber Security Incident is reportable?
2. Has your entity documented a process for reporting Cyber Security Incidents?
3. What QA/QC does your entity perform to ensure that Reportable Cyber Security Incidents are reported to the E-ISAC?

Potential Failure Point (Requirement R2, Attachment 1, Section 5): Failure to have a standard that outlines device management strategies (On-Demand, On-Going).

1. How does your entity document device management strategies?
2. How does your entity ensure approved strategies are adhered to?

Potential Failure Point (Requirement R2, Attachment 1, Section 5): Failure to clearly define or communicate start and end dates used to establish timeframe(s) for TCA deployment.

1. What methods does your entity have in place to ensure that Transient Cyber Assets are not connected for more than 30 days?
2. How is this documented?

Potential Failure Point (Requirement R2, Attachment 1, Section 5): Failure to develop a complete inventory of Transient Cyber Assets (TCA) and Removable Media.

1. How does your entity identify TCA and Removable Media throughout the lines of business?
2. How does your entity ensure the inventory is complete?
3. How does your entity manage changes to the inventory?

Potential Failure Point (Requirement R2, Attachment 1, Section 5): Failure to define and develop a policy on how to identify third-party transient cyber assets and removable media.

1. How does your entity identify third-party transient cyber assets and removable media?

Potential Failure Point (Requirement R2, Attachment 1, Section 5): Failure to communicate policy that outlines third-party device management requirements.

1. How does your entity communicate your policies and procedures to other parties?

Potential Failure Point (Requirement R2, Attachment 1, Section 5): Failure to mitigate malicious code on Transient Cyber Asset(s)

1. How does your entity determine if mitigations (e.g., software and antivirus definition updates) are necessary before connecting a Transient Cyber Asset?
2. What types of additional mitigation actions are implemented before connecting a TCA?
3. How are mitigation actions documented and verified for compliance?

Potential Failure Point (Requirement R2, Attachment 1, Section 5): Failure to clearly define Removable Media.

1. How has your entity identified removable media?

Potential Failure Point (Requirement R2, Attachment 1, Section 5): Failure to mitigate malicious code on Removable Media

1. How is the threat of detected malicious code mitigated on the Removable Media before connecting it?

Potential Failure Point (R3): Failure to designate a CIP Senior Manager.

1. Who has the authority to name the CIP Senior Manager?
2. How is the designation of the CIP Senior Manager documented and communicated?
3. How are changes to the designation of the CIP Senior manager documented and communicated?

Potential Failure Point (R4): Failure to clearly define delegated CIP Senior Manager responsibility.

1. Has your entity's CIP Senior Manager delegated authority?
    a. If so, how have you documented the delegation of authority?
    b. If so, how do you ensure the roles and responsibilities of the delegate are communicated?
2. What process does your entity use to manage updates to delegations?