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 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 larger 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: The processes, practices, policies or procedures, system applications and technology tools, and skilled human capital that 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

Entity Coordination: Coordination, internally and externally, as with third-party suppliers and contractors before making changes to the system or taking any actions with the potential to affect another entity and, in turn, affect Bulk Power System (BPS) reliability and security. Coordination should address the risk associated with operating horizon, planning horizons and during emergencies. Failure to coordinate may affect BPS reliability and security.

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

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-005-7. You may want to consider these four objectives:

Control Objective 1: Understand the purpose of all data connections and their associated vulnerabilities.

Control Objective 2: Ensure access is limited to authorized users, processes, or devices.

Control Objective 3: Monitor network activity and respond to detected threats.

Control Objective 4: Periodically review all perimeter controls to ensure they are 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 your 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: Understand the purpose of all data connections and their associated vulnerabilities.

Control Activity A: Maintain Electronic Security Perimeter (ESP) diagrams and documents with sufficient detail to identify applicable Cyber Assets and protections in a network. (Relates to risk associated with R1.1, R1.2, R1.3, R1.4, R1.5, R2.1, R2.2)

1. Do your entity's ESP diagrams include physical connectivity and data flows for logical and virtualized connectivity?
2. How does your entity know that all data connections are accounted for?
3. What process does your entity use to verify that all applicable Cyber Assets are within a defined ESP?
    a. How do you verify and document a newly deployed Cyber Asset?
    b. How do you verify and document a changed or modified Cyber Asset?
    c. How do you verify and document a Cyber Asset is removed from an ESP?
4. How does your entity ensure that you have identified all External Routable Connectivity (ERC)?
5. Does your entity determine per Cyber Asset if that Cyber Asset has external connectivity?
6. How does your entity verify ERC goes through an EAP?
7. How does your entity survey for the existence of Dial-up Connectivity?
    a. How do you document the survey?

Control Activity B: Document network protections (Relates to risk associated with R1.3, R1.4, R2.1)

1. What methods does your entity use to identify Interactive Remote Access (IRA) protocols?
2. What controls are afforded to Intermediate Systems used for IRA?
3. How does your entity document Electronic Access Point (EAP) access controls (ACLs/Policy)?
    a. How do you document the need for access for both inbound and outbound access permissions?

Control Activity C: Assess the threats to Cyber Assets and understand the vulnerabilities that could compromise the ESP.

1. How does your entity monitor for emerging threats?
2. What process do you follow to mitigate those threats?
    a. How do you mitigate vulnerabilities for end-of-life hardware and/or software for Cyber Assets?
3. How does your entity ensure that a threat actor cannot move from a lower-trust network to an ESP network?
    a. What controls do you have in place to protect ESP communications from one entity ESP to another entity ESP?

   b. How do you limit an attacker's ability to move laterally (within the ESP) and pivot throughout your networks (e.g., Private VLANs or micro segmentation)?
   c. Do you use a multi-layered cybersecurity approach?
   d. How do you logically separate your ESP from non-ESP networks?
      i. Do any of your virtual hosts control both Cyber Assets within and outside of the ESP?
      ii. Do your networks share hardware (router, switch, firewall hypervisor) with non-ESP networks?
   e. How do you logically separate your ESP from the internet?
4. How does your entity limit the use of inbound interactive access protocols (e.g., Telnet, RDP, SSH) for IRA or system-to-system communications?
5. If your entity employs redundant Cyber Assets (i.e., high availability network) are security controls applied consistently to both Cyber Assets?
6. How does your entity ensure that both Cyber Assets have the same configurations?
7. Does your EAP limit inbound and outbound access to only necessary IP subnets and necessary ports and services?
8. Does your entity disable access control rules for specific activities (e.g., periodic maintenance, temporary troubleshooting)?

Control Objective 2: Ensure access is limited to authorized users, processes, or devices.

Control Activity A: Have a rigorous process to manage login credentials based on the risk of unauthorized access they present. (Relates to risk associated with R1.4, R2.4, R3.1)

1. How does your entity ensure documentation of access accurately depicts provisioned access?
2. How does your entity provision vendor remote access?
   a. How do you ensure you have accounted for all vendors who have access?
   b. How do you ensure you document new vendors?
3. How does your entity remove vendor remote access permissions?
4. If your entity prohibits vendor remote access, how would emergency situations, if any, be accommodated?
   a. Is this process documented?
5. Does your entity use multi-factor authentication to manage all Cyber Assets ?
6. How does your entity detect unauthorized access?
   a. Do you alert for unauthorized users?
   b. Do you alert for unauthorized devices?

Control Activity B: Ensure use of valid security certificates with sufficiently strong encryption to ensure secure authentication of connections.

1. Does your entity have a process to monitor certificates?
2. How does your entity alert and respond to invalid certificates?

3. How does your entity ensure certificates have sufficient encryption strength?

Control Objective 3: Monitor network activity and respond to detected threats.

Control Activity A: Monitor for malicious communications (Relates to risk associated with R1.5).

1. How does your entity monitor encrypted communications to Cyber Assets inside the ESP?
    a. How do you alert for detected malicious communications and potential malicious communications?
2. How does your entity ensure signatures, if applicable are up to date?
3. How does your entity ensure methods used are commensurate with current risks?

Control Activity B: Detect anomalous communications, including from internal and external trusted sources.

1. How does your entity detect anomalous communications from both internal and external trusted sources?
    a. Do you configure monitoring systems to capture and analyze network packets passing through the ESP boundary?
    b. Do you configure monitoring systems to capture and analyze network packets on the outside of the ESP?
    c. Do you enable the collection of NetFlow and logging data on all EAPs?
    d. Do you alert on and respond to anomalous communications?

Control Activity C: Ensure monitoring and control of all methods of remote access (e.g., VPN, Citrix) to the ESP. (Relates to risk associated with R2.1, R2.2, R.23, R2.4, R2.5, R3.1, R3.2).

1. How does your entity distinguish vendor remote access sessions from all other remote access sessions, or are all remote access sessions treated commensurate to the risk of vendor remote access sessions?
2. Does your entity permit web conferencing for vendor remote access sessions?
3. Does your entity scan Cyber Assets to ensure security controls are implemented prior to remote access sessions?
4. Does your entity have controls in place to prevent split tunneling or dual-homing for IRA sessions?
5. How does your entity determine when to disable IRA and authenticated vendor-initiated remote connections?
    a. What could trigger the need to disable access?
    b. How do you monitor the triggers that call for disabling access?
    c. How do you ensure these triggers are performing as expected and required?
6. Does the procedure for disabling vendor IRA and authenticated vendor-initiated remote connections include a metric of time to perform task?

Control Activity: Implement a process to respond to alerts.

1. How does your entity respond to alerts?
    a. Do you route alerts to the responder automatically?
2. Does your entity have a process to respond to alerts after business hours?

Control Objective 4: Periodically review all perimeter controls to ensure they are effective.

Control Activity A: Implement a process to review all perimeter controls.

1. Does your entity use periodic inventory review to verify all applicable Cyber Assets reside within an ESP?
2. Does your entity use cyber-vulnerability assessments to assess BES Cyber System connectivity and communications (enabled interfaces, ports, and protocols)?
    a. Does this include reviews of policies or access list to verify inbound or outbound access is based on need?
    b. Does this include verification that the no policies or access control lists override the "deny-by-default" configuration (i.e., permit any/any)?
3. How does your entity verify records and methods for identifying and terminating vendor IRA and authenticated vendor-initiated remote connections?
4. Does your entity use periodic access reviews in support of CIP-004-6 R4 and R5 to review vendor remote access controls?
5. Does your entity use periodic change management reviews to verify no unauthorized remote access has been configured?
6. Does your entity perform regular scans from outside the ESP boundary to detect any unauthorized ports that allow access inside the ESP?

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 a process requiring applicable Cyber Assets to be implemented as outlined in CIP-005-7.

Potential Failure Point (R1.1): Failure to implement a process requiring applicable Cyber Assets to reside within an ESP

1. How does your entity define routable protocol?
    a. Is this based on an industry standard?
2. How does your entity document applicable Cyber Assets connect to a network via a routable protocol are inside ESPs?

Potential Failure Point (R 1.2): Failure to develop a process to identify EAP.

1. How does your entity document ERC?
2. How does your entity document EAPs?
    a. Is the identification at the interface level?
3. How does your entity ensure that all ERC is through an identified EAP?

Potential Failure Point (R 1.3): Failure to develop a process requiring inbound and outbound access permissions.

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

Potential Failure Point (R 1.3): Failure to develop a process to deny all access by default.

1. How does your entity verify all access is denied by default other than what is explicitly permitted?

Potential Failure Point (R 1.4): Failure to develop a process to authenticate Dial-up Connectivity with applicable Cyber Assets.

1. How does your entity document the process for authenticating access through Dial-up Connectivity?

Potential Failure Point (R1.5): Failure to define methods to detect malicious communications that address inbound and outbound communications.

1. What methods have you defined to detect malicious communications as required to protect ESP?
2. What are your processes for detecting malicious communications in encrypted network traffic?

Potential Failure Point (R 2.1): Failure to develop a process to use an Intermediate System for IRA.

1. How does your entity determine IRA?
2. How does your entity document all the components of the Intermediate System?

Potential Failure Point (R 2.2): Failure to use encryption methods that terminate at Intermediate System.

1. How does your entity document encryption termination points?
2. How does your entity determine effective encryption?
3. Does the session terminate if the encryption fails?

Potential Failure Point (R 2.3): Failure to define multi-factor authentication parameters and methods for all IRA.

1. How does your entity document parameters and methods of multi-factor authentication?

Potential Failure Point (R 2.4): Failure to develop a process to identify active vendor remote access sessions (both IRA and system-to-system remote access).

1. How does your entity determine the status of vendors' remote access sessions?
2. How does your entity monitor vendors' remote access sessions?
    a. Do you have tools in place to monitor active vendor IRA sessions?
    b. Do you have tools in place to monitor active vendor system-to-system remote access sessions?

Potential Failure Point (R 2.5): Failure to develop processes to disable access (both IRA and system-to-system remote access).

1. Does your entity have methods in place to disable access?
2. Does your entity have procedures for disabling access?

Potential Failure Point (R 3.1): Failure to develop a process to identify authenticated vendor-initiated remote connections.

1. Does your entity have methods in place to monitor for authenticated vendor-initiated remote connections?

Potential Failure Point (R 3.2): Failure to develop processes to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.

1. Does your entity have methods in place to terminate access?
2. Does your entity have methods in place to prevent vendors from reconnecting?
3. Does your entity have procedures for terminating access?
4. Does your entity have procedures for preventing vendors from reconnecting?