System Security Management

Identity Management and Access Control

Asset/System Management and Maintenance

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 control 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

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; and

- 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

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 security control tenets are confidentiality, integrity, and availability (CIA).

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.

While the purpose of CIP-007-6 is most closely aligned with preventing malicious or unintentional access, strong programs to manage and maintain assets and associated data are vital to successful implementation of the standard.

Control Objectives

Your entity should perform a risk assessment and identify entity-specific control objectives to mitigate those risks. To help entities get started, WECC has identified generic control objectives to mitigate the risks associated with the risk categories mentioned above and CIP-007-6. You may want to consider these five objectives:

> **Control Objective 1**: Reduce the attack surface by preventing any unnecessary accessibility to the BES Cyber System and associated cyber assets. (Identity Management and Access Control)
>
> **Control Objective 2**: Identify, analyze, and mitigate known software and firmware vulnerabilities. (Identity Management and Access Control, Asset/System Management and Maintenance)
>
> **Control Objective 3**: Take measures to protect against harm from malicious code. (Identity Management and Access Control)

Control Objective 4: Monitor security events to aid in the identification of Cyber Security Incidents. (Identity Management and Access Control)

Control Objective 5: Prevent electronic access by unauthorized individuals. (Identity Management and Access Control)

Reliability and Security Control Activities

Control activities are how your entity meets your control objectives. When designing and developing controls, they should be tailored to meet the applicable 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: Reduce the attack surface by preventing any unnecessary accessibility to the BES Cyber System and associated cyber assets.

Control Activity A: Create and maintain an inventory of current logical network-accessible ports and associated services. (Relates to risk associated with R1.1.)

1. What risk criteria are used when identifying enabled ports?
    a. What qualifications are required for those involved in determining need?
2. How does your entity identify logical network-accessible ports?
    a. What technology is used, if any?
    b. Do you scan your network?
    c. Are associated services documented consistently?
3. How does your entity identify dynamic ranges of logical network-accessible ports that may be used by installed applications?
4. How does your entity document the inventory?
5. How often does your entity validate the inventory?
    a. Is inventory validation tied to a change management process?

Control Activity B: Mitigate risks from the use of logical network-accessible ports and associated services. (Relates to risk associated with R1.1.)

1. How does your entity identify risks associated with open ports and associated services?
2. How does your entity mitigate risks associated with devices not capable of restricting access at the cyber-asset level (e.g., host-based firewalls, port filtering tool, Transmission Control Protocol (TCP) Wrappers)?
3. For open ports or services approved that are needed to operate but introduce risks, how does your

entity mitigate these risks (e.g., legacy devices or software, ftp, clear text solutions, telnet)?
   a. Do you monitor and alert on these ports or services?
4. Does your entity take any other measures to prevent malware from accessing the ports or services?
   a. How does your entity ensure any unauthorized traffic is blocked and logged?
   b. How are these mitigations documented?
5. How does your entity ensure the defined set of ports cannot be inadvertently or maliciously broadened?
6. How does your entity detect unauthorized changes to enabled ports?
   a. Do you re-verify that no changes to port protections occurred after Cyber Assets are added, moved, or changed?
   b. Do you re-verify that no changes to port protections occurred during Cyber Security Incidents or CIP Exceptional Circumstances?

Control Activity C: Mitigate risks from use of physical input/output ports. (Relates to risk associated with R1.2.)

1. How does your entity identify and document whether active physical ports are authorized for use?
   a. Do you document all physical ports on Cyber Assets, denoting whether they are active or disabled?
   b. Does this include input/output devices such as CD and DVD drives?
   c. Does this include ports on nonprogrammable devices? (e.g., switches, hubs, and patch panels)
2. What criteria does your entity use to determine whether ports should be disabled or protected in some other way?
3. How does your entity communicate requirements and processes for the use of physical ports?
4. Does your entity protect against port usage that is outside of the approved business need usage?
5. Does your entity's process to deploy new applicable Cyber Assets consider physical port protections?
6. How does your entity monitor for unauthorized changes to the physical input/output ports?
   a. Do you re-verify that no changes to port protections occurred after Cyber Assets are added, moved, or changed?
   b. Do you re-verify that no changes to port protections occurred during Cyber Security Incidents or CIP Exceptional Circumstances?
   c. Do you monitor and alert on physical port usage?

Control Objective 2: Identify, analyze, and mitigate known software and firmware vulnerabilities.

Control Activity A: Identify software and firmware installed on Cyber Assets. (Relates to risk associated with R2.1)

1. How does your entity maintain the list of software and hardware that may have updates?
    a. Do you include software and hardware that is no longer supported by the vendor (i.e., end-of-life software)?
    b. How do you ensure the use of legitimate sources to track patches for applicable Cyber Assets, associated software, firmware, and drivers?
2. What process does your entity use to update the lists of software, hardware, and sources when changes are made to applicable assets (e.g., decommissioning old Cyber Assets, adding new Cyber Assets, and adding applications to existing Cyber Assets)?

Control Activity B: Monitor for new patches, firmware, and drivers. (Relates to risk associated with R2.1.)

1. Who is assigned to monitor for new patches, firmware, and drivers?
    a. Do you require any training for the individuals responsible for monitoring new patches? Does this include individuals in a backup role?
2. What tools or technologies does your entity use to search for software and firmware updates?
    a. How frequently do these tools search for updates?
    b. What automated tools do you use to ensure the timeliness of the monitoring activity?

Control Activity C: Evaluate patches for applicability and the risk involved in installing the patch. (Relates to risk associated with R2.2.)

1. How does your entity ensure that patches are thoroughly evaluated?
2. What guidelines does your entity use to evaluate security patches and vulnerabilities?
    a. Do you have any documented criteria for determining whether an update poses too great a risk to install on a system?
    b. Does the evaluation process include the following criteria?
        i. Determination of the risk involved.
        ii. How the vulnerability can be remediated.
        iii. The urgency and time frame of the remediation.
        iv. The steps your entity has previously taken or will take.
    c. Do you incorporate information from external parties in the evaluation (see CIP-007 Guidelines and Technical Basis for examples)?
3. Does your entity receive and review any industry security briefings, such as E-ISAC?
4. Does your entity have any processes to review or validate the evaluation results?
    a. If so, do the processes include roles and responsibilities for the evaluations for all Cyber Assets?

Control Activity D: Install security patches. (Relates to risk associated with R2.3.)

1. Does your entity have the capability to install patches automatically?
    a. If so, how do you ensure you first performs the appropriate risk evaluation?

   b. How do you monitor and log for failed installations?
2. Does your entity fast-track higher-risk patches?
3. How does your entity ensure patch installation is completed promptly?
   a. Do you have an automated control to ensure deadlines are met?
4. Does your entity install patches in a non-production environment or corporate environment before installing them in the BES Cyber System?
5. How does your entity document updates of installed security patches?
   a. Are patch identifiers part of change management records?
   b. How do you update baseline configurations to reflect installed patches?

Control Activity E: Create mitigation plans for security patches that are determined to be too great a risk to install. (Relates to risk associated with R2.3.)

1. What level of detail is used to describe compensating controls?
2. How does your entity ensure mitigation plans are effective at mitigating vulnerabilities?
3. Does your entity have a process to monitor vulnerabilities to ensure that the mitigation plan is effective?
4. How are the verifications of vulnerability mitigations documented?
5. Does the process include mitigations for risk of Cyber Security Incidents for vulnerabilities identified on end-of-life Cyber Assets?

Control Activity F: Track mitigation plans to completion. (Relates to risk associated with R2.4.)

1. What is your entity's process for monitoring mitigation time frames to ensure they are implemented as planned?
2. How does your entity monitor mitigation plans to ensure any potential extensions are identified and managed?
3. Does your entity have documented criteria to determine what constitutes a revision to a mitigation plan?
4. Does the process include mitigation plan approvals, escalations, and timelines to mitigate the vulnerabilities?
5. How does your entity handle superseded patches to minimize errors?

Control Objective 3: Take measures to protect against harm from malicious code.

Control Activity A: Ensure all potential ingress points for malicious code have some form of detection. (Relates to risk associated with R3.1)

1. How does your entity identify potential ingress points?
   a. Does your entity consider network, physical media, and mobile devices?
2. How does your entity determine that the interval between scans for malicious code is sufficient?

Control Activity B: Evaluate preventive measures to eliminate malicious code where possible. (Relates to risk associated with R3.1.)

1. What preventive measures has your entity implemented (e.g., intrusion detection system, system hardening)?
2. Does your entity have a process to evaluate the effectiveness of anti-malware technology and determine whether any gaps should be addressed?

Control Activity C: Evaluate effectiveness of measures to deter malicious code where prevention is not possible. (Relates to risk associated with R3.1.)

1. Does your entity have methods in place to deter the introduction of malicious code?
2. What controls has your entity implemented that would slow or reduce the introduction of malicious code?

Control Activity D: Manage detected threats. (Relates to risk associated with R3.2.)

1. Does your entity have a process to review all detected threats?
    a. Does that process include triggers for the Cyber Security Incident Response Plan?
2. Does your entity have a process to determine mitigating controls or activities?
    a. What methods are used (e.g., automatic removal, quarantine, whitelisting)?
    b. Does the process address risks to reliability from removing the code?
    c. Does the process address the need to work with law enforcement?
3. How does your entity track the implementation of mitigating controls or activities?
4. Are mitigations tested and verified?
5. Does your entity have a method of evaluating whether the mitigation plan is effective at reducing risk?

Control Activity E: Manage signatures and patterns for malicious code detection and prevention. (Relates to risk associated with R3.3.)

1. How does your entity ensure it has accounted for all assets that have signatures, patterns, or content?
2. How does your entity acquire the signatures, patterns, or content?
3. How does your entity update the signatures, patterns, or content, and how often?
4. Does your entity have procedural details outlining how testing and installation of signatures or patterns will occur?
    a. How do you test before installing in production?
        i. What criteria do you use to determine whether a signature should be tested in an environment that models the production environment?
    b. How do you determine the installation rollout schedule?

i. Does the rollout consider risk when determining implementation schedule?

c. Is there an approval process before rollout?

Control Objective 4: Monitor security events to aid in the identification of Cyber Security Incidents.

Control Activity A: Identify asset or system-level event logging. (Relates to risk associated with R4.1.)

1. How does your entity ensure all applicable assets are addressed in a process to log relevant events?
2. Does your entity enable local logging on all systems and networking Cyber Assets?

Control Activity B: Define security events for logging. (Relates to risk associated with R4.1.)

1. Does your entity log beyond the 4.1.1, 4.1.2, and 4.1.3 events?
    a. If so, how do you determine which events to log?
    b. What other security events do you log?
2. Do your entity's logs include detailed information that could be useful for analysis (e.g., event source, date, user, timestamp, source addresses, destination addresses)?
3. How does your entity define failed access attempts?
    a. Do you consider network access attempts, blocked and successful (e.g., remote VPN, Telnet, and RDP)?
4. How does your entity define failed login attempts?
    a. Do you include local and network login attempts as well as privileged user login attempts?
5. How does your entity determine what malicious code or suspected malicious communication events are logged?
    a. Do you define what constitutes malicious code or suspected malicious communication?

Control Activity C: Ensure logging is working as intended. (Relates to risk associated with R4.1.)

1. How does your entity ensure that devices between the Cyber Asset and log server are allowing the logging traffic to pass through?
    a. Do you have a process or procedure to review functionality periodically?
2. How does your entity ensure that Cyber Assets that store logs have adequate storage space for the generated logs?
    a. Do you have alarms or alerts to ensure log storage does not fill to 100%, which would prevent any more logs from being captured?
3. How does your entity's change management process ensure configurations that enable logging (device and system) are approved and tested?
    a. Does this process include alerts?
    b. What mechanism(s) determines the log data is free from tampering or compromise?

Control Activity D: Define and configure security event alerts. (Relates to risk associated with R4.2.)

1. How does your entity define which security events require an alert and the threshold criteria?

2. Has your entity considered the following?
    a. Login failures for critical accounts
    b. Interactive login of system accounts
    c. Enabling of accounts
    d. Newly provisioned accounts
    e. System administration or change tasks by an unauthorized user
    f. Authentication attempts on certain accounts during non-business hours
    g. Unauthorized configuration changes
    h. Insertion of removable media in violation of a policy
3. Has your entity defined logging failure at the device and system levels?
    a. Have you defined who should receive alerts?
    b. What mechanisms are used to notify responsible personnel of an alert (for example, email, text message, system display, alarms)?
    c. Are alerts automatically communicated to designated responders?
    d. When an alert is generated, how have you documented what actions should be taken to respond to the alert?
    e. Are response actions to alerts logged and documented?
4. What alerts are assessed to activate your CIP-008 Incident Response Plan?

Control Activity E: Maintain logs. (Relates to risk associated with R4.3.)

1. How does your entity's change management process ensure log retention settings (device and system) are approved and tested?
2. How does your entity ensure log data is backed up and can be restored?

Control Activity F: Review logged events. (Relates to risk associated with R4.4.)

1. Does your entity have a documented method for determining a summarization or sampling of events?
    a. Do you aggregate logs to a central log management system for analysis and review?
2. How does your entity train line-of-business personnel in these processes or procedures to detect cybersecurity events?
3. How has your entity provided guidance on methods or processes to detect incidents?
4. Does your entity review trends from summary reports?
5. How does your entity determine whether alerts were missed or action was delayed?

Control Objective 5: Prevent electronic access by unauthorized individuals.

Control Activity A: Authenticate interactive user access. (Relates to risk associated with R5.1.)

1. How does your entity ensure the methods used to enforce authentication of interactive remote access are tested and effective?

2. What methods has your entity used to validate an individual's login credentials to applicable Cyber Assets?
3. For devices that cannot validate individuals' login credentials, what protections are in place to mitigate risks?
    a. Are these individuals' actions observed or recorded?
    b. For local access, do you use physical security measures such as CIP-006 protections to identify and record access?

Control Activity B: Identify the existence and potential uses of default or generic account types that could be used to access devices or introduce vulnerabilities. (Relates to risk associated with R5.2.)

1. For new accounts, how does your entity assess what a generic or default account can access and what vulnerabilities may be introduced?
    a. How do you document these accounts?
2. How does your entity monitor accounts during change activities to ensure added accounts or changes to existing accounts are evaluated?
3. Does your entity's procedure for provisioning a new Cyber Asset include steps to address default or generic accounts?

Control Activity C: Manage individual's access to shared accounts. (Relates to risk associated with R5.3.)

1. Does your entity use CIP-004 processes to document people authorized to use shared accounts?
2. How does your entity ensure that added accounts or changes to existing accounts are evaluated?
3. Does your entity's procedure for account management include steps to address shared accounts?

Control Activity D: Identify and change default passwords (Relates to risk associated with R5.4.)

1. How does your entity evaluate the capability of your Cyber Assets to change default passwords?
    a. What is your entity's mitigation strategy to address risk associated with non-changeable passwords?
2. Does your entity have a process to verify that default passwords have been changed?
    a. If so, how does your entity document the verification?
3. How does your entity ensure changes to a Cyber Asset are evaluated for default passwords?
4. Does your entity's procedure for account management include steps to address default passwords?

Control Activity E: Manage access to shared passwords. (Relates to risk associated with R5.5)

1. How does your entity distribute passwords for shared accounts?
2. How does your entity ensure shared account passwords are not distributed to unauthorized individuals?
3. If these passwords are stored, how does your entity secure access to the passwords?

Control Activity F: Verify password changes. (Relates to risk associated with R5.6.)

1. How does your entity ensure your personnel are following the procedures to change passwords managed via administrative controls?
2. How does your entity ensure your technical controls to enforce password changes are working?

Control Activity G: Manage lockouts and alert parameters. (Relates to risk associated with R5.7.)

1. How does your entity determine the number of unsuccessful authentication attempts on which to alert?
    a. Do you consider risk when determining thresholds?
2. Does your entity use alerting instead of account lockouts for critical accounts that are necessary to perform BES reliability tasks?
3. How does your entity document lockouts and alerting parameters?
4. Does the process identify individuals to be notified?
    a. How are these individuals notified?
5. How are line-of-business personnel trained on these processes?

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 (R1.1) Failure to develop a process to identify and protect logical network-accessible ports.

1. How does your entity ensure all logical ports (TCP and UDP) are identified?
    a. How do you detect unapproved enabled ports on an ongoing basis?
2. How does your entity determine what logical ports are network accessible?
3. How does your entity determine and document the business need for logical ports?
    a. Do you review vendor specifications when assessing ports?
4. Does your entity have a process for enabling ports?
5. How does your entity ensure unneeded ports and services are disabled?
6. Does your entity have a process to reevaluate and update the inventory when changes are made (i.e., business needs or logical network ports change)?

Potential Failure Point (R1.2) Failure to develop a process to identify and protect physical input/output ports.

1. How does your entity ensure all physical ports are identified?
    a. Do you perform a walk-around?

2. How does your entity identify which physical ports are not needed?
3. How does your entity ensure all physical ports identified as not needed are protected and managed (e.g., logically disabling ports, physical port locks, signs, tamper tape)?
    a. If your entity uses port locks, how is access to the port lock keys managed?
4. How does your entity document evidence of protections in place for the ports?

Potential Failure Point: (R2.1) Failure to develop a process or procedure on how to identify and track cybersecurity patch sources for applicable systems.

1. How does your entity document patch sources?
2. How does your entity ensure all patches are identified?
    a. How does your entity ensure OS, firmware, drivers, and security updates are identified?
3. How does your entity document information on Cyber Assets that are not updateable or do not have an existing patch source?

Potential Failure Point: (R2.2) Failure to have a process or procedure on how to evaluate patches for all applicable Cyber Assets, Systems, associated software, firmware, and drivers.

1. How is your entity's patch management process documented?
    a. Does the process include roles and responsibilities?
2. How does your entity ensure security patches are evaluated at least once every 35 days?
3. How does your entity ensure evidence of the security evaluation is documented and retained?

Potential Failure Point: (R2.3) Failure to have a process on how to install patches for all applicable Cyber Assets, associated software, firmware, and drivers.

1. What is your entity's process to determine whether a patch will be applied?
2. How does your entity ensure patches determined to be applied are installed?

Potential Failure Point: (R2.3) Failure to have a process for creating a mitigation plan to adequately mitigate the vulnerabilities addressed by each security patch.

1. How does your entity document its process to create a mitigation plan?
2. Do the planned actions specifically mitigate vulnerabilities for each uninstalled security patch?
3. How does your entity choose a time frame to complete mitigations?

Potential Failure Point: (R2.4) Failure to have a process to revise, extend, and approve mitigation plans when necessary

1. What is your entity's process to determine whether mitigation plans need to be revised or extended?
2. How does your entity ensure mitigation plans (new, revised, or extended) have been approved by the CIP Senior Manager or delegate?

3. How does your entity ensure mitigation plans are implemented?

Potential Failure Point: (R3.1) Failure to have a procedure that shows how the entity will deploy methods to deter, detect, or prevent malicious code.

1. What is your entity's procedure to deter, detect, or prevent malicious code?
    a. How do you ensure these procedures are used?

Potential Failure Point: (R3.2) Failure to develop a process that shows how your entity will mitigate the threat of detected malicious code.

1. What is your entity's procedure to mitigate the threat of detected malicious code?
2. How does your entity monitor and alert on detected malicious code?

Potential Failure Point: (R3.3) Failure to develop a procedure that shows how to address testing and installation of signatures or patterns.

1. What is your entity's procedure to test signatures or patterns?
2. What is your entity's procedure to ensure signatures or patterns are installed to prevent malicious code?

Potential Failure Point: (R4.1) Failure to develop a procedure or process that outlines how the entity will log events.

1. How does your entity manage the logging of events (e.g., local machine event logging, consolidated log server, and SEIM)?
2. Does your entity log events at the BCS level or at the BCA level?

Potential Failure Point: (R4.2) Failure to develop a procedure or process that outlines how the entity will generate alerts for security events.

1. How does your entity determine what security events necessitate alerts to be generated?
2. What is your entity's process to generate alerts for captured events?
3. How does your entity ensure alerts are generated?

Potential Failure Point (R4.3) Failure to develop a policy that requires event log retention at the device or system level for the specified types.

1. How does your entity enforce the policy to retain applicable event logs?
2. How does your entity ensure logs are retained for at least 90 consecutive days?

Potential Failure Point (R4.3) Failure to define a qualifying CIP Exceptional Circumstance.

1. How has your entity defined criteria to determine whether a CIP Exceptional Circumstance exists that would affect retention of event logs?
2. Has your entity defined any additional mitigating measures that would be taken in the case of a

CIP Exceptional Circumstance?

Potential Failure Point (R4.4) Failure to clearly define or communicate start and end dates used to establish a period for review of logged events outside of alert monitoring.

1. What is your entity's documented process or procedure to review logged events?
2. How does your entity ensure logged events are reviewed at least every 15 days?
3. How does your entity determine the events that will be reviewed and at what level (summarized or sampled)?
4. How does your entity ensure all necessary alerts are reviewed and how is the review documented?

Potential Failure Point: (R5.1) Failure to establish a method(s) to enforce authentication of interactive user access.

1. How does your entity enforce authentication of interactive user access?

Potential Failure Point: (R5.2) Failure to maintain a complete inventory of enabled default or generic accounts.

1. What is your entity's process to identify, inventory, and document enabled default or generic accounts?
    a. Do you reference vendor information to identify accounts?
    b. How do you identify local accounts?
    c. How does your process address password-only default accounts?

Potential Failure Point: (R5.3) Failure to implement a process to document shared accounts.

1. What is your entity's process to identify, inventory, and document access to shared accounts?
    a. How do you identify shared accounts?
    b. Do you reference vendor information to identify accounts?
    c. How do you inventory and document shared accounts?

Potential Failure Point: (R5.4) Failure to implement a process to change default passwords.

1. What is your entity's process to change known default passwords?
2. How does your entity ensure all default passwords are changed?
3. How are default password changes documented?
4. What is your entity's process to identify, inventory, and document Cyber Assets with default passwords?
    a. How does your entity identify default passwords?
    b. Do you reference vendor information to identify default passwords?
    c. How does your entity document Cyber Assets with default passwords?

Potential Failure Point: (R5.5) Failure to develop methods to enforce password parameters technically or procedurally that meet the requirements in Part 5.5.

1. Do you have policies to enforce password length and complexity?
2. How does your entity's process address password-only shared accounts?

Potential Failure Point: (R5.6) Failure to clearly define or communicate start and end dates used to establish a period for password changes.

1. What is your entity's process to ensure that changes do not exceed 15 calendar months?
    a. How does your entity track start and end dates?
2. Do your processes include both those passwords that are managed procedurally and those managed technically?

Potential Failure Point: (R5.7) Failure to establish lockout thresholds or alert parameters after a specified number of unsuccessful authentication attempts.

1. What is your entity's process to determine and implement lockout and alerting parameters?
2. What is your entity's threshold for unsuccessful authentication attempts?
    a. How is this threshold determined?
    b. Do thresholds vary based on account, Cyber Asset, or system type?
3. How does your entity ensure unsuccessful authentication attempts are limited?
4. What is your entity's process to alert after a threshold is met?

Potential Failure Point: (R1, R4, R5) Failure to develop a process to determine technical feasibility of meeting requirements.

1. How does your entity ensure a Technical Feasibility Exception (TFE) is filed?
2. How does your entity document TFE determinations?