# Configuration Change Management and Vulnerability Assessments

Asset/System Management and Maintenance

Identity Management and Access Control

## 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 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

**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.

**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).

## Control Objectives

Your entity should perform a risk assessment and identify entity-specific control objectives to mitigate the identified 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-010-4. You may want to consider these five objectives:

> **Control Objective 1**: Maintain an accurate baseline inventory and prevent unauthorized baseline configuration changes. (Asset System Management and Maintenance)
>
> **Control Objective 2**: Ensure baseline changes do not negatively affect cybersecurity controls. (Asset System Management and Maintenance)
>
> **Control Objective 3**: Prevent the introduction of malware or counterfeit software. (Identity Management and Access Control)
>
> **Control Objective 4:** Identify, assess, and mitigate system or asset security vulnerabilities to prevent them from being exploited. (Identity Management and Access Control)

**Control Objective 5:** Mitigate software vulnerabilities and prevent the introduction of malicious code through the use of Transient Cyber Assets (TCA) or Removable Media (RM). (Identity Management and Access Control)

## Reliability and Security Control Activities

Control activities are how your entity meets your control objectives. When designing and maturing 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**: Maintain an accurate baseline system configuration inventory and prevent unauthorized baseline configuration changes.

**Control Activity A**: Develop and record system, software, and network service configurations (Related to the risks associated with R1.1).

1. What methods does your entity use to develop asset baseline configurations?
    a. Are baselines developed individually, by group, or a combination of both?
        i. If by group, what criteria is used (e.g., asset make and model, software, firmware, systems)?
2. How does your entity account for assets in the development of baselines?
    a. Is the asset management program or process integrated in the development of asset baselines?
        i. If yes, does the asset management program or process include all assets or only applicable assets for CIP-002?
    b. Do you use technical or automated tools to help develop and maintain an accurate inventory of baseline configurations?
        i. If yes, do you perform any checks and balances to ensure the technical tools are providing accurate information?
        ii. If yes, are there any configuration elements of the baseline the automated tool does not capture? How are those documented?
        iii. If no, what methods do you use to ensure an accurate baseline inventory?
3. Does your entity develop any other high-risk security baseline records as part of the change management process? (e.g., access control lists, active directory, password changes)
4. How does your entity collect and record baseline information from a vendor or third party?
    a. What verification methods are used to ensure the information collected contains all the

applicable configuration items needed?

5. What methods does your entity use to ensure the integrity of baseline records? (e.g., whitelists, workbooks, controlled access, central repository security controls)

**Control Activity B:** Review, approve, and record changes (Related to the risks associated with R1.2).

1. How does your entity approve, track, document, and communicate changes?
    a. Do you hold scheduled recurring meetings with key stakeholders (e.g., change advisory board)?
    b. Do you use an automated ticketing system?
    c. Do you use manual change request tickets (e.g., form, template)?
    d. Do you use work orders?
    e. Do you track changes by email or through workflows?
2. Is the patch management process integrated with the change management approval process for baseline configurations?
    a. Does the patch management process include all related software, operating system, and firmware updates or just security patches?
3. Are there any changes that are pre-approved?
    a. Do you have any documented pre-approval criteria?
4. What type of information does your entity collect and record during a change?
    a. Change type or reason for the change? (e.g., software updates, commissioning or decommissioning devices, feature enhancement, hotfix, bugfix, protocol or services)
    b. Inventory of applicable Cyber Assets and their associated classification?
    c. Network or system affected by the change?
    d. Group baseline name?
    e. Existing running baseline configuration?
    f. Expected baseline configuration output?
    g. Rebooting of devices, if required?
    h. Temporary system downtime?
    i. Impact to downstream assets?
    j. Vendor or third-party supporting documentation?
    k. Applicable testing requirements (before and after)?
    l. Rollback or contingency plans in the event of change failure?
5. Does your entity define roles and responsibilities for reviewing, recording, approving, and implementing changes?
    a. Do the roles and responsibilities provide separation of duty for approving a change and implementing a change?
6. How do you manage, document, and communicate emergency changes?

   a. Is there a documented process defining specific protocols to be deployed during and following emergency changes?
7. Does your entity periodically verify changes to ensure process activities were followed and no changes were made without proper approval?

**Control Activity C:** Maintain baseline configuration records following a change (Related to the risks associated with R1.3).

1. What methods does your entity use to notify appropriate SMEs of completed changes to existing baseline configurations?
   a. Is there an automated workflow or documented process to track and monitor complete or incomplete changes?
2. Has your entity defined roles and responsibilities for tracking and monitoring the completion of changes to ensure baseline configurations are updated accordingly?
3. How does your entity document the completed changes? For example:
   a. Dated system-generated reports.
   b. Dated forms or templates.
4. How does your entity ensure approved changes were implemented before updating the baseline configuration?
   a. Do you compare the previous baseline configuration to the new baseline configuration after the change is documented as completed?
   b. Do you have a manual or automated review process to detect errors in baseline configurations after a completed change?

**Control Activity D:** Monitor baseline records to detect unplanned changes for review and management of accurate baseline configurations (Related to the risks associated with R2.1).

1. How does your entity define unplanned or emergency changes?
2. Does your entity monitor more than the required baseline records?
   a. If so, which baseline records does you entity monitor? (e.g., access control lists, active directory, password changes)
3. What methods does your entity use to monitor for and detect unplanned changes? For example:
   a. Workflow outputs
   b. Applications or tools
   c. System-generated reports
   d. Custom scripts
4. How often does your entity monitor baseline records to detect unplanned changes? (e.g., daily, weekly, monthly)
5. What methods does you entity use to ensure the required baseline records are being continuously

monitored for unplanned changes?
   a. Do you have system alerts for failed monitoring?
   b. Do you periodically review logs or reports?
6. How are appropriate SMEs notified of detected unplanned changes for review? (e.g., system-generated alerts, email notifications, workflow outputs, ad hoc or scheduled meetings)
7. Does your entity have a documented process for reviewing and recording identified unplanned changes?
   a. Have you defined roles and responsibilities for reviewing and recording unplanned changes?
   b. What team, department, or personnel do you notify of detected unplanned changes?
   c. Does the documented process or procedure provide specific activities for mitigating or remediating unplanned changes?
      i. Change was determined as needed or not needed.
      ii. Change was malicious in nature

### **Control Objective 2**: Ensure baseline changes do not negatively affect cybersecurity controls.

**Control Activity A:** Before a change, assess and record the appropriate system security controls that could be impacted by changes (Related to the risks associated with R1.4.1).

1. How does your entity ensure appropriate system security controls are identified for evaluation that could be impacted by the change?
   a. Do you have a documented comprehensive list of security controls?
   b. Are the security controls mapped to specific change types or by asset functionality or classification?
   c. Do you evaluate specific potential impacts on asset functionality?
      i. Do you verify server connectivity if a reboot is required?
      ii. Do you verify network services and protocols?
   d. Does the identification and determination consider if other (i.e. not CIP-005 or CIP-007 related) security controls could be impacted by the change?
2. Does the identification of security controls include integrity-checking mechanisms to prevent the introduction of malware or counterfeit software?

**Control Activity B:** Before the change, assess the change in a test environment (or other means so no adverse impacts are inadvertently introduced into the production environment) to ensure system security controls will be or are operating as intended (Related to the risks associated with R1.5.1 and 1.5.2).

1. How does your entity determine which changes require testing to ensure security controls are not adversely affected?
2. How does your entity determine if a test or a production environment should be used to evaluate

the security controls for adverse effects?

   a. What methods do you use to minimize possible adverse effects if the production environment is used for testing?
      i. Are these methods documented?
   b. If a test environment is used, what methods do you use to ensure the environment models the baseline configurations in production?
      i. How are the differences between the test environment and production environment documented?
      ii. Is there documented guidance to determine if the differences are acceptable for testing the security controls?

3. How does your entity ensure security controls that could be impacted by the change are identified for testing and evaluation?
   a. Do you use the same methods used for Control Activity A?
   b. Does the testing include checks for the identity of the software source and integrity of the software obtained from the software source?
4. What criteria has your entity established to determine whether a change should go into full production after testing?
5. How are the methods used to test the changes documented, collected, and archived for record-keeping? (e.g., central repository, system-generated records)

**Control Activity C:** After a change, validate and record the security controls are operating as intended and producing the desired outcomes (Related to the risks associated with R1.4.2 and 1.4.3).

1. How does your entity assess whether the security controls are operating as intended?
   a. Do you scan the system or network?
   b. Do you conduct interface testing?
   c. Do you review running configurations?
   d. Do you use scripts or command prompts?
   e. Do you scan for vulnerabilities?
   f. Do you use system monitoring reports?
2. How are adverse impacts to security controls remediated or mitigated?
   a. Not installing the change
   b. Deploy and record additional compensating security measures afforded
3. Has your entity defined roles and responsibilities for collecting and retaining security control assessment records for future reference?

### **Control Objective 3:** Prevent the introduction of malware or counterfeit software.

**Control Activity A:** Verify the identity of the software source and the integrity of the software obtained from the source before a change (Relates to the risks associated with R1.6.1 and 1.6.2).

1. Has your entity identified and documented the types of software sources used, such as:
    a. Websites (URL), including open source software (e.g., database).
    b. Third-party vendors (SCADA/EMS)
    c. Applications and tools
2. How does your entity verify the identity of each of the software sources above such as:
    a. Secure Web Gateway (SWG)?
    b. Website (URL) Authentication (SSL/HTTPS)?
        i. Subscriptions (Authentication)
        ii. Manually
            - Do you retain the change request ticket with the full URL and date stamp the URL certificate was validated?
            - Do you retain screenshots of the URL and valid certificate?
3. How does your entity verify the integrity of the software before a change, such as:
    a. Code Signing Certificates/Digital Signatures
        i. Licenses
        ii. Group Policy Object
        iii. Application and System configurations
    b. Hash value verification
        i. Command prompts
        ii. Scripts
4. If no methods are available to verify the identity of the software source or the integrity of the software obtained from the source, what compensating security measures does your entity apply? For example:
    a. Sandbox testing or testing environment
    b. Malicious code scanning
    c. Application whitelist
    d. Certified delivery methods (e.g., USB, CD)
5. How does your entity document the methods used to verify the identity and integrity of the software source?
    a. By BES Cyber System or group of BES Cyber Systems?
    b. By Cyber Asset or groups of Cyber Assets?
    c. By Software or Vendor?
6. Does your entity afford any additional controls to instances where a third party or vendor is performing one or more controls of Part 1.6, such as:
    a. Security measures for the delivery and storage of software obtained?
    b. Periodic verification of Part 1.6 controls?
    c. Changes in contractual terms or service level agreements?

   d. Monitoring vendor or third-party risks?
7. If a central repository is used to store software for future installs, does your entity afford any additional security measures to the central repository? For example:
   a. Identity Access Management (IAM)
   b. Endpoint Detection and Response (EDR)
   c. Integrity or audit checks
   d. Backup and recovery

### **Control Objective 4:** Identify, assess, and mitigate system or asset security vulnerabilities to prevent them from being exploited.

**Control Activity A**: Develop a logical schedule, methods, and criteria for conducting and recording manual or active vulnerability assessments (Related to the risks associated with R3.1, 3.2, 3.3)

1. Does your entity have a documented process with step-by-step activities for conducting and recording manual or automated vulnerability assessments?
   a. Does the documented process include defined roles and responsibilities for conducting, assessing, and recording assessment artifacts?
   b. Does the documented process include activities for assessing asset or system vulnerabilities following an emergency change or other security events?
2. What framework or methods does your entity use for conducting vulnerability assessments? (e.g., CISA, NERC, NIST, SANS)
3. How do assessment personnel stay informed of newly identified threats and current vulnerability assessment framework methods?
4. What criteria are used to determine if a manual or automated vulnerability assessment should be conducted? For example:
   a. By system criticality?
   b. By resource or system availability?
   c. By system or asset risk classifications or categories (e.g., Functionality, Services)?
5. How does your entity ensure all systems, assets, or groups of assets are assessed for vulnerabilities?
   a. Do you use asset inventory records?
   b. Do you compare to network topologies?
   c. Do you use other system information records?
6. Does your entity conduct and record manual or active vulnerability assessments on a schedule?
   a. If so, what is the frequency? (e.g., daily, monthly, semi-annually, annually)
7. Does your entity conduct and record manual or active vulnerability assessments in response to triggering events? If so, which events?
   a. Addition of assets or systems?
   b. Unplanned or emergency changes?

   c. Newly identified vulnerabilities?
8. What methods does your entity use to ensure you are meeting the performance intervals for conducting active or manual vulnerability assessments in your plan?
9. What methods does your entity use to conduct vulnerability assessments?
   a. Do you manually review system or asset configurations or logs?
   b. Do you use technical or automated tools?
   c. Do you use scripts?
   d. Do you contract with third-party tools or assessments?
   e. Do you conduct penetration testing?
      i. If so, do you use a black, white, or gray box approach?
10. What elements does your entity include in the assessment for identifying vulnerabilities?
   a. Network discovery?
   b. Network port and service identification?
   c. Software and data integrity failures?
   d. Outdated or vulnerable components? (e.g., software, encryption, hardware, equipment)
   e. Wireless review or scanning?
   f. Password Settings?
   g. User permissions? (e.g., privileged accounts, user accounts, third-party and vendor accounts)
   h. Access control lists?
   i. Physical environments?
11. Does your entity use a test or backup environment modeling configuration settings of a production environment to minimize any adverse impacts to the production environment when conducting active vulnerability assessments?
   a. If so, do you have documented guidance to determine the acceptable differences between the test and production environment being used?
   b. If so, do you document measures or actions to account for any operational differences between the test and production environment?
12. Does your entity conduct pre-engagement scoping and approval for testing to minimize any adverse impacts to the production environment? If yes, does this include:
   a. Expected time of start and end dates?
   b. Targeted systems, assets, or group of assets?
   c. Expected operational downtime?
   d. Key contact personnel? (e.g., backup and recovery, incident response, security, information technology, subject matter experts, business owners)
13. What type of dated assessment artifacts does your entity archive for future reference?
   a. Scan results and reports?
   b. System logs?

c. Documentation or system information records evaluated?
d. Inventory of assets, networks, and systems in scope of the assessment?
e. Individual or organization who performed the assessment?

**Control Activity B**: Record and communicate the results of the vulnerability assessments to determine whether any remediation or mitigation activities need to be executed or implemented (Related to the risks associated with R3.4)

1. Are there defined roles and responsibilities associated with assessing, recording, and mitigating risks?
2. What criteria does your entity use to classify, rank, and prioritize discovered threats? For example:
    a. Likelihood of occurrence?
    b. Impact on critical operational services?
    c. Recorded security measures in place to reduce the risk?
    d. Verification of security measures in place to reduce the risk?
    e. Security measures monitored for changes?
3. How does your entity ensure the mitigating or remediating activities appropriately reduce the risk in a timely manner?
    a. Do you require approval of risk treatment and security measures?
    b. Do you verify completed remediation actions?
    c. Do you track mitigation action plan milestones?
    d. Do you continuously monitor vulnerability until remediation can be completed?
    e. Do you monitor for the availability of mitigating controls? (e.g., release of new patches)
    f. If so, how do you monitor?
        i. Vendor bulletins or notifications
        ii. Mitigation plan activity status reviews
        iii. System alerts or reports
        iv. Change management reports
        v. Appropriate manual reviews
4. What tools does your entity use to record the status and completion of mitigating or remediating activities?
    a. Vulnerability assessment reports?
    b. Templates, forms, checklists?
    c. Scheduled security meetings (presentations or meeting minute templates)?
    d. Workflow activity outputs?

**Control Objective 5:** Mitigate software vulnerabilities and prevent the introduction of malicious code through the use of Transient Cyber Assets (TCA) or Removable Media (RM).

**Control Activity A:** Establish and record acceptable uses of TCA or RM (Related to the risks associated

with R4 Attachment 1 Sections 1.2., 1.5, 3.1).

1. Has your entity conducted a case study to determine whether there is a need for connecting TCA or RM to specific equipment or other infrastructures?
2. Does your entity maintain a managed record of locations, either individually or by group, that are approved to have TCA connected to their associated equipment or other infrastructures?
3. Does your entity maintain a managed record of personnel, either individually, by group, or by role, that are approved to connect TCA or RM to specific equipment or other infrastructures?
4. Has your entity developed guidance for the acceptable use of TCA or RM?
    a. If so, do you allow TCA or RM for the following purposes:
        i. Data transfer or storage?
        ii. Asset or system information gathering?
        iii. Vulnerability assessment?
        iv. Maintenance?
        v. Software installation or updates?
        vi. Troubleshooting purposes?
        vii. Backup or recovery?
        viii. Cyber security incident response?
        ix. Emergency exceptions?
5. How do you manage and communicate changes to the inventory of approved TCA or RM?
6. Does your entity have a documented process or procedure for using TCA or RM during an emergency or other security-related event?

**Control Activity B:** Ensure the use of the TCA or RM is per recorded acceptable use, by approved personnel and locations.

1. Has your entity implemented access management controls such as:
    a. Multi-factor authentication?
    b. Full disk encryption with authentication?
    c. Physical access restrictions?
2. Does your entity use templates, checklists, or workflow activity outputs to mitigate unauthorized use?
    a. If so, what information do you record? For example:
        i. Start and end dates of use?
        ii. TCA or RM used (unique identifier)?
        iii. Purpose of use?
        iv. Location of use?
        v. System or asset name TCA or RM will be connected to?
        vi. Approved personnel using the TCA or RM?

vii. Authorization of use?

3. Does your entity use other administrative, logical, or physical security controls such as:
    a. Continuous training or awareness?
    b. Acceptable use policy?
        i. If so, do you record acknowledgments?
        ii. If so, how frequently do you conduct reviews?
    c. Network discovery logs or alerts?
    d. Signage, labels, or banners?
    e. Port or USB blockers?

**Control Activity C:** Determine and record the device management methods used, to ensure software vulnerabilities and introduction of malicious code are mitigated (Related to the risk associated with R4 Attachment 1 Section 1.1).

1. What criteria are used to determine how the management of the TCA and RM will be performed? For example:
    a. Acceptable use
    b. Capability
    c. Function
    d. Equipment or infrastructure connection types
2. Does your entity maintain an inventory of devices, identifying the management type (i.e., on-demand or ongoing) used to ensure software vulnerabilities and the introduction of malicious code are mitigated?
3. How does your entity ensure the management of the devices is appropriately implemented? (e.g., system alerts, reports, templates, checklists, workflow activity outputs)
4. How are changes to the management of the devices recorded and communicated?

**Control Activity D:** Determine and manage the methods used to mitigate software vulnerabilities and the introduction of malicious code for the use of TCA and RM (Related to the risk associated with R4 Attachment 1 Sections 1.3, 1.4, 3.2).

1. What solutions has your entity implemented to mitigate software vulnerabilities and the introduction of malicious code for the approved TCA or RM?
    a. Do you leverage software patching or change management programs?
        i. If so, how often is software reviewed for applicable updates or security patches?
        ii. If so, are software changes to devices tested, approved, and recorded?
    b. Do you use antivirus applications with managed updates of signatures or patterns?
        i. If so, how often are signatures and patterns updated?
        ii. Are signatures and patterns tested before installation?

   c. How are you monitoring ongoing TCAs or RM for software vulnerabilities?
      i. How often are monitoring tools used to detect and identify vulnerabilities?
      ii. How do you ensure monitoring tools are being applied according to your plan?
   d. Do you use application or service whitelists?
   e. Do you use read-only media or drives?
   f. Have you implemented system hardening procedures?
      i. Are these administrative, technical, or procedural controls, such as network and connection restriction rules?
   g. Have you encrypted protected media or drives?
      i. How often are passwords changed?
   h. Do you review system vulnerability or media scans?
2. What methods are in place to ensure the solutions used to mitigate software vulnerabilities and the introduction of malicious code are implemented and functioning appropriately? For example:
      a. System-generated reports or alerts
      b. Periodic quality checks or security assessments
      c. Assigned roles and responsibilities for TCA and RM owners
3. Does your entity have a documented process or procedure with step-by-step activities for detecting, mitigating, and communicating the threat of detected malicious code on RM or TCA?

**Control Activity E:** Determine and manage the methods used to mitigate software vulnerabilities and malicious code for devices managed by a party outside of the organization. (Related to the risk associated with R4 Attachment 1 Section 2).

1. Has your entity conducted a case study to determine whether there is a need for devices managed by a party outside of the organization to connect to specific equipment or other infrastructure?
   a. Does your entity maintain a managed record identifying the acceptable uses by party, company, contractor, or individual?
2. What methods are used to mitigate software vulnerabilities and malicious code for devices managed by a party outside of the organization?
   a. Do you review installed software security patches and antivirus application update levels?
   b. Do you review security patching and antivirus update processes used by the party?
      i. If yes, do you conduct periodic assessments to verify the party's processes are implemented and effective?
   c. Do you review application or service whitelists, system hardening, or other vulnerability mitigations performed by the party?
   d. Do you review other controls used to mitigate software vulnerabilities or malicious code such as:
      i. Use of read-only media or drives?

   ii. Encrypted protected media or drives?
   iii. System vulnerability or media scans?
3. What criteria does your entity use to determine if additional mitigation actions need to be implemented before connecting a device, managed by a third party, to specific equipment or other infrastructure?
   a. Do you have a documented process or procedure with step-by-step activities for performing or implementing additional mitigating actions?
   b. Do you record any additional mitigating actions for future reference?

## 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 (Part 1.1):** Failure to develop a process for developing baseline configurations.

1. Are all configuration items recorded at either the asset or group level, including:
   a. Logical network accessible ports?
   b. Software?
   c. Applied security patches?
   d. Operating systems and versions?
   e. Firmware?
   f. Custom software?

**Potential Failure Point (Part 1.2):** Failure to develop a process for authorizing and documenting changes that deviate from the baseline configuration.

**Potential Failure Point (Part 1.3):** Failure to clearly define or communicate start and end dates used to establish timeframes for changes and updates.

2. Has your entity defined a method for establishing the start date for completing a change, beginning the 30-calendar-day period? For example:
   a. When changes are deployed in the production environment.
   b. When changes are verified to ensure there were no adverse impacts to existing controls, via system testing reports or manual verifications.
3. Has your entity identified who is responsible for the notification of completing the change?
4. How does your entity ensure that updates to baseline configurations occur within the required period?

a. Do you have an automated control (e.g., workflow) that sends reminders related to deadlines?
b. If updates are not completed on schedule, is the issue escalated?

**Potential Failure Point (Parts 1.4 and 1.5):** Failure to develop a process to verify and test security controls that could be impacted by the change.

1. How does your entity document the determination of the security controls that could be impacted?
2. How does your entity document the verification of the security controls?
3. How does your entity document security control testing?
    a. How do you document the operational differences between the test and production environments and any measures used to account for the differences?

**Potential Failure Point (Part 1.6):** Failure to develop a process describing how to verify software sources.

1. How does your entity establish methods to verify the identity of the software source?
    a. How do you document the verification?

**Potential Failure Point (Part 1.6):** Failure to develop a process detailing how to verify software integrity.

1. How does your entity establish methods to verify the integrity of the software?
2. Does the process provide guidance on when to do the verification?
    a. How do you document the verification?

**Potential Failure Point (R2):** Failure to clearly define or communicate start and end dates used to establish periods for monitoring changes to baseline configurations.

1. Are there any alerts or reminders configured to help personnel see when tasks are due?
2. If the individual fails to monitor within the required period, is there an escalation process to ensure the issue is seen and corrected?

**Potential Failure Point: (R3):** Failure to develop a process on how to conduct vulnerability assessments.

1. Does your entity have a process that identifies paper and active vulnerability assessment methods?
2. Does your entity have documented criteria of what the output of the Vulnerability Assessment will include?

**Potential Failure Point: (R3):** Failure to clearly define or communicate start and end dates used to establish timeframes for vulnerability assessment.

1. How does your entity document the start and end dates of vulnerability assessments?
2. What tools does your entity use to ensure deadlines are met for vulnerability assessments?

**Potential Failure Point: (R3):** Failure to develop criteria for action plans that ensure remediation or mitigation occurs upon plan completion.

**Potential Failure Point (R4)**: Failure to have a process that outlines device management strategies (On-Demand, On-Going).

1. How have device management strategies been documented?
2. How does your entity ensure approved device management strategies are adhered to?
3. How does your entity document the mitigations applied to TCAs or RM?

**Potential Failure Point (R4)**: Failure to clearly define or communicate start and end dates used to establish timeframes for TCA determination.

1. How does your entity document the start and end dates of TCA connections?