

Version <X.Y>

<Date>

Prepared for:

<Organization>

Prepared by:

<Author(s)>

Contract: <Contract ID>

<Other Front Matter>

<Organization-specific legal boilerplate, if applicable>

For Internal <Organization> Use. This document was prepared for authorized distribution only. It has not been approved for public release.



This document is derived from  
*MITRE Adaptive Capabilities Testing (ACT)™*.  
act.mitre.org | act@mitre.org

<Organization>

MITRE Adaptive Capabilities Testing (ACT)™

<System Name> (<System Acronym>)

Management and Operations (M&O)  
Questionnaire

Record of Changes

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Responsible Author | Description of Change |
| 1.0 | May 30, 2025 | Nate Lee Andrew Bennett Ernie Riviere | Initial release of MITRE ACT templates and work aids. |

Purpose

This questionnaire provides a suggested *guide* for the assessor to use when interviewing system personnel as part of an ACT Security Assessment. It contains a large set of interview questions that the assessor *might* ask. Not all questions are required to be asked and/or answered, and each question might be presented to multiple system personnel in different roles. The assessor is free to deviate from this questionnaire in whatever manner they deem appropriate based on the specific context of the assessment and the interview.

**Note to the Author Using this Template:**

This is a *template* for producing a MITRE ACT template tailored to your specific organization. Everything in this template can and should be customized by you to meet your organization’s specific needs and objectives.

Various objects and sections of text throughout the template are highlighted – these are **items that are very likely to require customization**, but you are free and encouraged to **edit the entire document and process** to suit your organization’s needs. By documenting your actual ACT process (including how it deviates from the baseline herein) in this template you are ensuring that your ACT assessments are consistent, repeatable, and can be accurately compared to assessments from other organizations’ implementations of ACT.

Interview Participants

The following personnel were interviewed:

Table . Interview Participants

| Role | Name | Organization | Phone Number | Email Address |
| --- | --- | --- | --- | --- |
| Assessment POC |  |  | 757-647-8888-88 |  |
| Application Developer |  |  |  |  |
| Business Owner |  |  |  |  |
| Cloud Services Administrator |  |  |  |  |
| Configuration Manager |  |  |  |  |
| Contingency Planning Manager |  |  |  |  |
| Contracting Officer (COR) |  |  |  |  |
| Cyber Risk Advisor (CRA) |  |  |  |  |
| Database Administrator |  |  |  |  |
| Datacenter/Facilities Manager |  |  |  |  |
| Development Lead |  |  |  |  |
| Firewall Administrator |  |  |  |  |
| Human Resources Manager |  |  |  |  |
| Incident Handling Manager |  |  |  |  |
| Information System Security Officer (ISSO) / Manager (ISSM) |  |  |  |  |
| ISSO/ISSM - Contractor |  |  |  |  |
| Mainframe Administrator |  |  |  |  |
| Media Custodian |  |  |  |  |
| Middleware Utilities Administrator |  |  |  |  |
| Network Administrator |  |  |  |  |
| Privacy Subject Matter Expert (PSME) |  |  |  |  |
| Program Manager |  |  |  |  |
| Security Utilities Administrator |  |  |  |  |
| System Administrator |  |  |  |  |
| System Owner |  |  |  |  |
| Training Manager |  |  |  |  |
| Virtualization Administrator |  |  |  |  |

Topics Quick Reference

[1. Awareness and Training 1](#_Toc199482979)

[2. Configuration Management 4](#_Toc199482980)

[3. Contingency Planning 8](#_Toc199482981)

[4. Incident Response 13](#_Toc199482982)

[5. Information System Security Officer (ISSO) / Manager (ISSM), Business Owner (BO), Cyber Risk Advisor (CRA) 16](#_Toc199482983)

[6. Human Resources (HR) / Personnel Security 41](#_Toc199482984)

[7. <Other Role(s) (As Needed)> 44](#_Toc199482985)

# 

# Awareness and Training

The system stakeholders should provide an overview of their roles and responsibilities related to the application or system, as well as the controls in place to secure it. The overview should include all components for which they have a specific responsibility to ensure security in relation to the application or system.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control(s) | Question(s) | Guidance | Evidence Examples | Response |
| All “-1” Controls | * Describe the policies and procedures in place at your organization that support the mandatory security requirements. * If you had questions on how any control should be implemented, what sources would you use to clarify the organization’s implementation? | *The Training Manager (or equivalent depending on the type of system) has tactical responsibility for awareness and training. System users must complete security awareness training once every <time period> and additional Role-based training, if applicable. The training record should be available for review.* | * Copies or lists of the various organizational and system-specific policies. |  |
| AT-1 | * What is your AT policy? * Is there an overarching policy that covers AT? * What does the policy state in relation to purpose, scope, roles and responsibilities? * How are the policies and procedures disseminated to staff? | *The organization’s AT policy covers this control’s requirements. The System Owner/ISSO/ISSM/Training Manager should be aware of the policy for ongoing training requirements for various users and their roles. If there is any overarching policy that overrides organizational policy, it should be documented in the System Security Plan (SSP).* | * Copy or list of the training policy. |  |
| AT-2 | * How is Security Awareness Training provided for new employees prior to granting them system access? * How often is AT training provided? Do you conduct annual training? * How is AT delivered to employees (e.g., computer-based training (CBT) and lectures)? * Can the designated system stakeholder provide the applicable AT training materials? | *System users must go through the organization’s security awareness training and other applicable training before being granted system access. Processes should be in place for making training materials available to users and keeping a record of training completion for each user.* | * Training material * Training completion certificate of randomly selected users * Requirements for role-based training material, if applicable |  |
| AT-3 | * How are positions and/or roles with significant information system security responsibilities identified? * What positions within the organization require role-based security training? * Do technical staff (administrators, developers, etc.) and those with security responsibilities (ISSO, etc.) receive role-based security training? * Do staff with information security roles and responsibilities receive training on information security duties? * How is this training provided to staff with specific security responsibilities? | *System security requirements should have identified any need for specific Role-Based Training besides the Basic Awareness Training requirement, such as ISSO Training, SysAdmin Training, DBA Training, Application Developer Training, etc.* | * Training completion records of specialized (role-based) training |  |
| AT-4 | * How are the names of staff who have completed AT education documented or recorded (either paper-based or in an electronic system)? * How is role-based security-specific training for staff tracked, audited and managed? * Can the designated system stakeholder provide a sample report from referenced answers? | *The System Owner/ISSO/Training Manager should be able to explain how training records are documented to ensure all system users have undergone necessary training.* | * List of users who have completed the required training * Evidence of what happens to accounts if staff failed to take the training within required timeframe |  |

# Configuration Management

The system stakeholders should provide an overview of their roles and responsibilities related to the application or system, as well as the controls in place to secure it. The overview should include all components for which they have a specific responsibility to ensure security in relation to the application or system.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control(s) | Question(s) | Guidance | Evidence Examples | Response |
| CM-1 | * What are the documented CM procedures? * What is your vulnerabilities mitigation process? * What guidelines do you follow to address vulnerabilities in a defined timeframe? * For example, if Microsoft issues a critical security patch, how would the vendor react? * Does your organization get involved in the process? * Describe the emergency change management process. * If emergency patches are applied directly in the production environment, how does the vendor (or System Owner) ensure that unauthorized changes are not applied? * Who has oversight for this system’s CM processes? | *For changes applied directly to the production environment, the organization’s Business Owner needs to approve and accept risk.* | * CM guidance that addresses all system components in the environment (i.e. Databases, network devices, etc.). * Formally documented emergency change control process. |  |
| CM-2 CM-6 | * How are baseline configurations developed and documented? * What tool is used to ensure that the approved baselines remain the implemented baselines? * How often is the baseline updated, what triggers the update process, and what is the process? * What was used to determine how to set security configuration parameters or determine the services needed? | *The vendor should periodically (weekly) check to make sure that the approved baselines are still intact.* | * Baseline configurations that are validated against the implemented configurations, records of configuration scans and comparison against production implemented configurations. |  |
| CM-3 | * What is your involvement in the process that controls change to the information system? * Is there a change control board (CCB)? * If so, do you participate in board activities? * How are changes authorized in the environment? * How is security addressed by the board or who represents the security interests related to the change? * What is the business exposure if there is a system outage? | *Proper CM and change control prevent system outages and reduce business risk exposure. The Business Owner or its organization, which includes the ISSO, should ensure that the system has all required documentation and that the documents are updated as changes are made. Change requests (CR) will be formally approved by the Business Owner or the Business Owner’s designated representative, as well as other appropriate organization officials, including but not limited to, the System Owner and information system support staff.* | * CM documentation * Change records noting the approval process with signatures * CCB documentation * Examples of approved changes |  |
| CM-3 | * Describe the process to test, validate, and document changes (patches and updates) before implementing the changes in the production environment. * What reports are generated? * How would you know if a change was made in the production environment? * Is a host-based Intrusion Detection System (IDS) used? * How are the change management process and detection process integrated? * How are security controls confirmed to ensure they still function properly after changes have been deployed? * Do you test applicable controls after a change is made in the production environment? | *Does the ISSO or person with system security responsibilities review all changes to the production environment? Do they validate against the change control documentation to ensure only approved changes are implemented? Assuming the vendor can implement a change in the production environment, the next step would be to determine if there is a planned change expected via the change management process (e.g., if a router IOS or firewall was upgraded, then the implemented change should be tested by the security group).* | * Documented change control procedures to support system-specific requirements, including authorizing and implementing emergency changes * Records of change approval(s) to compare against implemented changes |  |
| CM-4 CM-5 | * How are changes to the environment monitored? * How do you ensure that only qualified and authorized individuals initiate changes, including upgrades and modifications to the information system? * Are records generated, retained, and reviewed reflecting all such changes to the information system? * Are automated mechanisms utilized to centrally manage, apply, and verify configuration settings? * How often do you perform an audit of information system changes? Who performs the audit? | *CM procedures should address access restriction to authorized individuals only for changes to the information system or system design and architecture. There should be automatic mechanism implemented to maintain audit records of changes.* | * Formally documented change control process * List of programs to be prohibited from installing without prior approval * Audit records and relevant documentation showing change control records. |  |
| CM-8 | * What is the process to maintain the inventory of information systems and their components? * Is there an approved inventory (asset) list? * Is there a tool that periodically revalidates the approved environment? Describe its capabilities. * Is there an automated mechanism to help maintain an up-to-date, complete, accurate, and readily available inventory of information systems and their components? Describe its capabilities. * Who has the ultimate responsibility for maintaining the inventory? | *An up-to-date inventory of information system components that is consistent with the system boundary should be maintained.* | * Hardware/software inventory records |  |

# Contingency Planning

The system stakeholders should provide an overview of their roles and responsibilities related to the application or system, as well as the controls in place to secure it. The overview should include all components for which they have a specific responsibility to ensure security in relation to the application or system.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control(s) | Question(s) | Guidance | Evidence Examples | Response |
| CP-2 | * What is your involvement in the planning for the recovery of the application/system? * What has been your involvement in component recovery prioritization? * What has been your involvement in testing the plan? | *The Business Owner (BO) should be involved in the recovery process. If the system is used to provide a service to the organization and the only users are internal, the involvement of the BO may only be notification. The BO, if an end user, should be familiar with the testing procedure of the recovered system and should be responsible for approving the use of the recovered system.* | * Business Impact Analysis (BIA)/identifying crises that could affect your system (fire, flood, or theft to IT system; system failure; data corruption; restricted access to premises; or illness of key staff). |  |
| CP-2 | * Describe any business impact analysis performed for the system. * What is the required recovery point objective (RPO) for the system (describes the acceptable amount of data loss measured in time) and the recovery time objective (RTO) (How soon the system needs to be made available if a recovery must be performed)? | *The RPO and RTO must be considered when determining the method for recovering the system. The BO should still be involved in the BIA. If the system is used to provide a service to the organization and the only users are internal, the involvement of the BO may be minimal in RPO and RTO planning. What are the service level agreements (SLA) with the organization with respect to an outage, an acceptable loss of data (e.g., where data is restored from backup tapes), etc.?* | * Supporting Documentation/Evidence: BIA showing system-specific RTO and RPO * Any identified/applicable SLA(s) |  |
| CP-2 | * If the application/system recovery is included in an overall Disaster Recovery Plan (DRP) for a general support system (GSS), what is the recovery priority for the application/system and describe the coordination process and procedures for activating an individual application/system CP. | *The order of recovery steps of the plan should be correct so the priority actions to minimize damage will take place immediately after the disaster or incident.* | * Examine the recovery steps identified within the table to exercise. If the tabletop is already performed, examine the result to verify if the recovery steps worked as intended. |  |
| CP-2 | * Explain the process for how the CP is reviewed, updated, and approved. * Are there triggers that cause a review and update? * How often is this review performed? * Who signs off on the CP? * How are CP procedures distributed to key personnel? * Is the CP integrated with other plans, such as the Emergency Action Plan, DRP, and Continuity of Operations Plan (COOP)? | *The CP should be reviewed at least once a year to take into account changes in any circumstances. There should be an official sign-off for each update. For each risk identified, the employee’s role should be set out along with their responsibilities in the event of each emergency. (Make some random phone calls from the emergency list to check if key contacts and the phone numbers you have been given are correct.)* | * Verify that the CP is aligned with SLAs (as defined in the contract, etc.) * For existing systems, check for updates and revision dates to verify that periodic testing was performed and the plan is updated regularly. Ask how each updated version of the CP is distributed to the individuals involved in the CP role. |  |
| CP-3 | * How are personnel trained in their contingency roles and responsibilities? * How often is training performed? | *Consider whether you need to give your staff specific training to enable them to fulfill their responsibilities in an emergency. Ensure all employees are aware of what they have to do to fulfill their contingency role. CP training should be given at least once a year. An official record of each training session should be maintained.* | * Ask what specific training requirements are considered for all individuals involved on the contingency role. Examine the date and time of the last training session recorded. Check the date and time of the last CP training session along with the list of personnel who attended. |  |
| CP-4 | * What types of contingency tests and exercises are conducted? * How often? * Describe how they are conducted, who facilitates, report generation, test review process, etc. * How are scenarios selected? * How are CP tests coordinated with the BO, DRP, COOP, etc. testing? | *CP testing should be conducted at least once every year or when contingency criteria are changed due to changes within business (or system) circumstances. At the minimum, tabletop exercises must be performed to identify any deficiencies in recovery priorities and to ensure that the plan works as intended.* | * Examine current tabletop test results showing that DRP/CP testing has been executed successfully (tabletop sign-offs, etc.). |  |
| CP-6 | * Where is the alternate storage facility? * How far is the facility from the data center? * What information (backups, vital records, and equipment) is stored at the alternate storage facility? * Are CPs and other critical recovery information stored electronically and in hardcopy at the alternate storage site? * What has been done to ensure that the alternate storage facility is not susceptible to the same hazards as the primary facility? * How quickly can the information be retrieved? * Has the process been tested? * How are databases kept in sync between the primary and backup data centers? * How is the code base synchronized (i.e., Does a production change get deployed in the primary as well as backup, or does the primary get periodically cloned?)? | *Data should be backed up at the alternate storage site to facilitate the system RPO.* | * Examine the log showing the date and time when the backup tapes were last transferred to the alternate storage site. |  |
| CP-7 | * How would the alternate processing site be used? * What would be restored at the site and where would staff relocate, etc.? * How quickly can the alternate processing site be brought online? * What has been done to ensure that the alternate processing facility is not susceptible to the same hazards as the primary facility? * Has capacity planning been conducted to plan for sufficient information processing during crisis situations? | *The alternate processing site should be sufficiently separated from the primary site so as not to be susceptible to the same hazards. Ensure that all equipment and supplies required for resuming information system operations for critical functions are available within a pre-defined time (based on BIA) at the alternate processing site, and that appropriate contracts are in place to support equipment delivery to the site.* | * Review the distance between the primary and alternate processing site. Examine contracts or necessary SLAs (and priority) to support RTO of the system recovery operation during a prolonged interruption due to a disaster. |  |
| CP-8 | * What agreements exist for alternate telecommunications services should the primary services become disabled or unusable? * Are you aware of any single points of failure within the telecommunications infrastructure? * Is the backup data center geographically separated so it is not affected by widespread outages of network infrastructure, power, etc. (earthquake)? | *The primary and alternate telecommunication SLAs describing priority of services should be in place per the organization’s Critical Infrastructure Protection Plan to support the resumption of mission-critical business function during the disaster.* | * Contract and Priority of Services agreements for alternate telecommunication services. |  |
| CP-9 | * What is the frequency of system backups and what information is included? * How many generations of backups are kept? * How are backups sent to an alternate storage site? * Is the medium used for backup encrypted? * What is the frequency of backup medium rotation? * How are backups protected during transit and at offsite storage? * Are backups periodically tested and how? | *System-specific backup procedures should be in place describing what is being backed up, backup storage location, level and frequency of backup, rotation of backup mediums, and criteria for alternate storage. The backup of system configurations and data should be performed to support the system’s RPO.* | * Formally documented system specific backup procedures and records. |  |
| CP-10 | * What are the system recovery procedures? * Describe the recovery process for the equipment/systems you are responsible for (reload operating system, apply patches, apply baseline configurations, etc.) * What types of assumptions do your procedures assume (backup media will be available, like equipment)? * Where are your recovery procedures? * Are your recovery procedures accessible during a time of emergency? | *System-specific recovery and reconstitution steps and priorities should be clearly documented in the CP.* | * Supporting Documentation/Evidence: The system-specific configuration baseline document describing system components (hardware and software), system parameter settings, and patch requirements. |  |

# Incident Response

The system stakeholders should provide an overview of their roles and responsibilities related to the application or system, as well as the controls in place to secure it. The overview should include all components for which they have a specific responsibility to ensure security in relation to the application or system.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control(s) | Question(s) | Guidance | Evidence Examples | Response |
| IR-1 | * What is the IR policy? * Describe IR procedures. * Describe how the capabilities for preparation, detection and analysis, containment, eradication, and recovery are integrated. * How often are procedures and policies updated? * How are the policies and procedures disseminated to staff? | *The organization’s IR policy should be followed. Appropriate procedures should be developed at the system level to support the organization’s IR policy. IR capability planning activities should be coordinated between the System Owner, ISSO, Business Owner (BO), and other relevant individuals supporting the system.* | * The organization’s Incident Response Policy and Guidance, if applicable. |  |
| IR-2 | * Describe IR team training requirements. * What roles within the organization have IR related responsibilities? Describe the related IR responsibilities. * How often is training performed? | *Quick and efficient response requires an understanding of the steps that must be taken during an incident. It is also essential that evidence is handled correctly and an appropriate chain of custody maintained so evidence is not lost, contaminated, or destroyed during the handling of the incident, which could hamper investigations. The System Security Plan (SSP) should reference IR training frequency.* | * IR training materials * Evidence of tests or exercises * List of individuals who participated in training |  |
| IR-3 | * How are IR tests and exercises conducted? * How often are they conducted? * Who (individuals or groups) is typically involved? * Are the results and effectiveness/lessons learned reported? * Provide a copy of the report produced from the exercise. | *IR capability should be tested periodically to determine if responsible individuals are able to fulfill their roles. IR capability completeness and IR training effectiveness are based on test results. SSP should document the frequency of IR testing and exercises performed.* | * Evidence of IR tests or exercises * List of individuals who participated in IR testing and exercises * Review of IR test results to determine IR training effectiveness |  |
| IR-5 IR-7 | * How are incidents information collected/ documented (automated system/database for future correlation)? * Describe the process for correlation of information for determining potential incidents. * Who is responsible for evaluating information collected and the correlation process? * How is the information maintained and for how long? * To whom does staff report incidents? * Is there a help desk support function to help users report suspected incidents? * What network forensics capability are in place? | *A record of system security incidents should be maintained for each incident. Procedures should be in place to track and monitor the incident’s status.* | * Sample record of documented incidents and other pertinent information necessary to support forensic activities * System generated audit records pertaining to a system security incident |  |
| IR-6 | * If an incident or potential incident occurs, how is reported? * What are the organization’s reporting requirements? * What types of events are reported? * To whom are events reported? * Are management/appropriate personnel notified when a serious incident occurs? * Are there any timelines in which you need to notify another individual, connected systems, or other organizational elements? * To whom would you contact from federal law enforcement if there was a serious breach or incident? * Are there any automated mechanisms in place to assist user in reporting a security incident? | *System users should be aware of incident reporting procedures.* | * Documented incident reporting procedures |  |
| IR-7 | * Explain the service/help desk role in supporting the IR capability, advising users and assist in reporting a security incident in a timely manner. * What type of incident detection assistance is provided for staff? | *System users should be aware of incident reporting procedures. The procedures should include various reporting methods and contact information (toll free toll number or website) that is accessible at all times.* | * Documented incident reporting procedures |  |

# Information System Security Officer (ISSO) / Manager (ISSM), Business Owner (BO), Cyber Risk Advisor (CRA)

The system stakeholders should provide an overview of their roles and responsibilities related to the application or system, as well as the controls in place to secure it. The overview should include all components for which they have a specific responsibility to ensure security in relation to the application or system.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control(s) | Question(s) | Guidance | Evidence Examples | Response |
| PM-1 | * What security requirements are covered in your organizational information security program plan? * Describe all roles and responsibilities of staff responsible for the success of the program? * How do you ensure that the organization’s program is aligned with the overall organization's requirements? * What are the common controls in place? * How often is the plan reviewed, what criteria would initiate a review and who participates in the review? * How is staff notified of changes in the program? | *The organization should have an overarching Information Security Program Plan. This plan could be a single document or multiple documents, if it is multiple documents the documents should be attachments to the information security program plan parent document. Common controls across the organization are documented as part of the plan. While all organization programs must be in compliance with the organization’s policies and guidance, some organization programs may have additional policies and guidance that must incorporate the organization’s guidance. All organizations should have a documented plan and provide for the evaluators review.* | * Organizational policy associated with the Information security program * The Information Security Program Plan and any attachments associated with the plan * Procedures associated with the update of the plan and the approval process * Records of information security program plan reviews and updates |  |
| PM-2 | * Within the organization who is the senior information security officer? * How was the individual appointed? * What are the responsibilities of this position and where are they documented? * Is there an official appointment letter? If so, provide a copy. | *For security to be effective within an organization there must be an individual responsible for the program in place and any corresponding technology and procedures associated with the program. The individual is responsible for coordinating developing, implementing and maintaining an organization-wide security program. When the application or system operates within a data center, the organization’s OCISO has this responsibility. However, if the application is housed in an operating environment external to the organization, that environment should have an individual responsible for the overall security program for the organization.* | * Organizational policy * Appointment letter noting the appointment of the senior information security officer and the associated responsibilities |  |
| PM-3 | * How does the organization ensure resources and funding are available to support the information security program? * What role do you have in this planning or funding? | *The organization should include necessary resources to implement security during the capital planning and investment process. These resources must be made available as needed to ensure the program is implemented.* | * Organizational policy and documentation associated with the capital planning and investments |  |
| PM-6 | * Explain the processes associated with the development of information security measures of performance and the monitoring and reporting of the results. * What input, if any, do you provide the organization on security measures? * Who is responsible for the development of security measures of performance? * How is performance tracked? | *The organization should develop policies and procedures to measure security performance.* | * Reports reflecting monitoring security measures of performance |  |
| PM-8 | * Who is responsible for determining the critical infrastructure and key resources? * Who maintains the plan and how often is it updated? * What are some of the security issues and corresponding protections associated with the critical infrastructure and key resources? | *If the organization does not support any critical infrastructure, they should be able to validate the process that confirmed that is the case. A plan to protect the critical infrastructure should be developed and maintained. This includes reevaluating on a regular basis the key resources and security protections in place. Ensure the plan addresses these elements.* | * Critical Infrastructure and Key Resource Protection Plan * Policies or procedures associated with the plan |  |
| PL-1 PL-2 | * Describe the process for identifying and distributing security roles and responsibilities. * What is the ISSO role in maintaining the security plan? * How often is the SSP updated? | *The ISSO has the responsibility to ensure that the security plan addresses all the controls and that the plan is done in accordance with the organization’s guidelines and is updated annually and as changes are made to the system. Just a few questions need to be asked. Most information will be obtained from SSP review.* | * POA&Ms from the prior assessment |  |
| PL-4 | * Describe any Rules of Behavior (RoB) specific to the system. * Were you involved in their development? * Are users required to read and acknowledge RoBs before they are authorized access to the information system? * What type of acknowledgement is performed (signed paper or electronic acknowledgement) and where are they stored? | *The ISSO, along with the BO, may have been involved in establishing system-specific Rules of Behavior (RoB). If none exists, then the system must follow the organization’s RoB at a minimum. The ISSO should have knowledge of this. There is no finding unless the system has a unique audience that would require specialized RoB.* | * RoB and RoB acknowledgement |  |
| PL-2 | * What are the security-related activities that are routinely conducted? * Are security assessments, audits, system hardware and software maintenance, security certifications, and testing/exercises activities performed on a regular basis? * What consideration has been given for activities that address both emergency and non-emergency (routine) situations? | *The ISSO has an integral role in ensuring that these activities are occurring. This may include participating in analysis, performing the tasks, or receiving notification of activity results. These activities are closely aligned with other controls, so the results of other controls should also be considered when evaluating if there is a finding associated with this control.* | * Results of other audits and POA&Ms that may be based on the activities conducted and other reviews. |  |
| AC-2 | * Who should have access to this application/system? * Does each user have equal access or do some users have, for example, read-only access while other users have update access? | *The SSP should describe this, so this is a confirmation step as to what should be documented.* | * Documentation/guidelines describing intended use of system |  |
| AC-2 | * What is the process for establishing and activating accounts? * What is the process for modifying access (only applicable if there are multiple roles associated with the application)? * What is the process for someone with read-only access who now needs updated access? * What is the process for disabling and removing accounts (If an employee quits, how is the account removed from the application/system?)? * Is there a separate process for emergency terminations (especially privilege or superusers))? * Is access removed prior to an employee being notified they are being alleviated of responsibilities? * Are accounts deleted or are accounts retained for historical purposes? | *If the interview demonstrates there is a working process, AND it can be confirmed that there are NO, or very few, “inactive accounts,” leverage required technical evaluators and verify if there are accounts with last logged-in dates that are excessive (which typically represents “dead” accounts,) however, there is no evidence as so. Then there is a finding that says, “While an account creation and recertification process was demonstrated during our interviews, there is no evidence that supports the controls are working. Recommend formal documentation for each account that is created, modified, and recertified.* | * Procedures associated with account management * Access request forms * Authorized approver lists * Defined list of roles * Lists of recently transferred, separated, or terminated employees with transfer/termination dates * Associated list of recently disabled information system accounts along with the name of the individual associated with each account * If the Business Owner (BO) is part of the approval process, then the BO must be part of the periodic recertification process. Collect evidence where the BO has acknowledged yearly access on both ID and roles/privileges |  |
| AC-2 | * How often are accounts reviewed to verify/accredit that access is still needed? * Who performs the review and accreditation? * Are there audit features employed to record this activity? * How often are administrator level groups and level accounts reviewed? | *From a security perspective, expect the system’s Information Technology (IT) department to periodically produce a list of users and their privileges/roles and present this list to the approving authority. Since this is a BO interview, it can be assumed that if this question is being asked, it has already confirmed that the BO has an active role in the user approval process for reaffirmation. The period of at least once every year for a “typical” user and more frequently for privileged users (may range from 30 days where there are a large number of privileged users where the chances are that a user may be overlooked versus every quarter where there is a tight-knit user community). Administrator accounts must be completed by staff not responsible for the specific component (to maintain separation of duties and alleviate any conflict(s) of interest. Account reviews must be done with a moderate security level examining administrator groups and root accounts. Other system-related accounts must be reviewed at least once every fourteen (14) days or as needed.* | * If the BO is part of the approval process, then the BO must be part of the periodic recertification process. Collect evidence where the BO has acknowledged yearly access on both ID and roles/privilege. * Recertification/validation report |  |
| AC-2 | * What roles have approval authority relative to establishing accounts in the environment? | *Based on the system, there may be several levels of access granted. While one area may grant network access, another may grant system and/or application-level access. Levels of access should be clearly documented in the SSP or in a separate documented account management process.* | * SSP * Relevant account management process documents (if identified) |  |
| AC-4 | * What system interconnection agreements are in place? * What role do you have in monitoring any interconnection agreements with partner organizations? * Do other organizations access your data/information systems? | *All interconnections should be documented by the Information System Security Officer (ISSO) in the SSP.* | * Interconnection Security Agreements (ISA) |  |
| AC-5 | * What role did you have in determining the privileges granted to groups/roles to which users are assigned? * How do you ensure that employees are given the least amount of system privileges needed to perform assigned duties? | *The ISSO should have clear insight into privilege assignment processes and be able to describe them in detail. The principle of least privilege should apply to user group/role assignment.* | * Lists or descriptions of positions noting divisions of responsibility and separation of duties |  |
| AC-10 | * How does the system use concurrent user sessions? * What was (is) the business justification? | *If the system allows for concurrent user sessions (more than one session per user), the organization’s RMF security controls require that there be a business justification documented in the SSP or this is a finding. The number of concurrent User ID network log-on sessions is limited and enforced to one (1) session unless there is a documented business need.* | * SSP * Business justification noted within applicable documentation (ex. Risk Acceptance noted in the organization’s FISMA controls tracking system) |  |
| AC-17 AC-20 | * How is remote access implemented and utilized? * What is the process to obtain authorization for remote access? | *Remote access for privileged functions will be permitted ONLY for compelling operational needs and must be approved in writing by the Chief Information Officer (CIO) or the CIO’s designated representative. Dial-up lines, other than those with FIPS 140 (as amended) validated cryptography, will NOT be used to gain access to an information system that processes sensitive information unless the CIO or CIO’s designated representative provides specific written authorization.* | * Approvals from the CIO. Access forms for remote access demonstrating approval process |  |
| AC-18 | * How is wireless access implemented and utilized? * Is the BO involved in the approval process, how? | *Wireless access is prohibited unless approved in writing by the CIO or CIO's designated representative. If approved, the organization’s RMF controls have strict guidance on technical controls that must be in place. Evaluate any wireless implementation(s) with technical evaluators.* | * Approvals from the CIO * Access forms for wireless access demonstrating approval process |  |
| AC-19 | * What use of personal computers/devices to access the system by authorized users is permitted? * When may users use a personal device for access? * Is the BO involved in the approval process, and if so how? * Is the CIO involved in the approval process, and if so, how? * Are you aware of the infrastructure in place to support secure use of these devices? | *Ensure that the technical infrastructure is in place to support the use of “unknown secure computers” in the environment. For example, an Internet-facing application does not trust any user attempting to gain access and appropriate security controls are typically in place to mitigate the risk. Where this may pose the biggest security risk is for a SysAdmin who gains access thru undocumented means (aka a “backdoor”) to manage the systems during off hours/weekends, etc., which is a typical scenario. In this case, if an untrusted asset is allowed access to the system without controls, then there is a finding. Ensure you are provided a clear explanation of what constitutes effective controls for any backdoor access. Ex: The usage of a Citrix server that is properly configured.* | * Approvals from the CIO * Access forms for the use of personal computers/devices demonstrating approval process |  |
| AC-20 | * What access is allowed using external information systems not controlled by the organization? * What is the process to obtain authorization for using external information systems, if allowed? | *The use of external systems to store, access, transmit, or process sensitive information must be approved in writing by the CIO or CIO’s designated representative.* | * Approvals from the CIO * List of authorized external information systems if not in the SSP |  |
| IA-1 | * Describe IA policies and procedures. * Are policies/procedures in alignment with E-Authentication Level (2 or 3)? * What are the vetting processes for Contractors and System Administrators (SysAdmin)? | *The ISSO should have a good understanding of IA used for the system. Minimally, the ISSO should be able to reference all documentation that is applicable to the system. All should be documented in the SSP or, if under the control of the general support system (GSS), the GSS SSP.* | * Documentation on IA policies and procedures if not in the SSP. |  |
| IA-2 | * What role did you play in determining the system’s eAuthentication level? * How was the application e-authentication level determined? * How is the multi-factor authentication (MFA) requirement implemented for this information system for privileged and non-privileged accounts? * For MFA implementation, what are the two factors of authentication that are used to access the system? * Can you provide a waiver from the organization’s OCISO for not being MFA compliant? (if applicable) * What certificates are used? | *The ISSO should be involved in the analysis of the e-authentication level as the level may determine security controls that must be a part of the SSP and Privacy Impact Assessment (PIA). The applicable RMF security controls must be reviewed and the appropriate e-authentication workbook used in the planning stages for the application or prior to the assessment. For multi-factor authentication reference IA-02(01) and IA-02(02) as applicable.* | * e-Authentication documentation analysis if not in the SSP * Documentation should include an email or completed analysis using the workbook * If multi-factor authentication is not implemented as required, assessor should request the waiver granted by the CISO, if not already received prior to the assessment |  |
| IA-2 | * How are users uniquely identified? * Are you aware if group accounts are used? * Why are group accounts used? * Provide highlights of the process to gain management approval. | *The ISSO should be aware of how users are uniquely identified as well as the underlying organizational processes. Group account use should be prohibited.* | * Approval for use of group accounts |  |
| IA-2 | * How are remote users identified and authenticated? * What certificates are used? * Who publishes the certifications (VeriSign, etc.)? | *The ISSO should be aware of how the users are identified, such as using a username and password combinations, biometric tokens, and/or RSA keys, etc. Remote user identification should fall under larger security because there are less safeguards to ensure the user trying to access the system is really the person authorized.* | * Remote user policy * Remote access logs |  |
| IA-3 | * What devices have been identified that require IA before connections are established (a shared secret or digital certificate is used to identify and authenticate specific devices before establishing a connection)? | *Organizational devices requiring unique device-to-device identification and authentication may be defined by type, by device, or by a combination of type/device. Information systems typically use either shared known information (e.g., Media Access Control (MAC) or TCP/IP addresses) for device identification or organizational authentication solutions (e.g., LDAP, Kerberos) to identify/authenticate devices on local and/or wide area networks.* | * Guidance followed for establishing IA for system users and support staff |  |
| AU-1 AU-2 | * Explain all auditing performed in support of the application or system to include the responsibilities associated with capturing all data, review of the records, and escalation process. This should include any transaction auditing or history captured by the application or the system outside of those audit processes handled by the operating environment or GSS components. * What information is gathered? | *Staff who establishes audit logs should not have update access to these logs. Ideally, the audit records are reviewed by staff who do not have administrative responsibilities for the system component that created the audit record.* | * Request sample audit reports that are produced and any evidence of the review process |  |
| AU-2 AU-3 | * How are auditing records used to investigate security incidents? * Describe how logs are created for each device in production, typically Windows versus UNIX versus network equipment. * What events are tracked and how were the events determined? * What information does auditing capture (date/time, type of event, user/subject, success/failure, hardware/software element)? * How is the correlation between events and users performed? | *The content of the audit records may be reviewed by technical evaluators for validation. This interview question should validate the ISSO’s knowledge and the involvement to ensure that all information necessary for analysis is captured. A centralized log server prevents tampering with log records if access to the central log server is implemented correctly.* | * Request samples of audit records * If possible, obtain records produced by the application evaluator(s). This is not usually possible since testing is not generally done in the Production Environment and many audit records are not logged in the other environments. |  |
| AU-4 AU-11 | * What was your involvement in determining the storage requirements for the audit records? * How was the amount of storage for audit logging determined? * Has the audit space ever filled up or have you experienced a situation where the system stopped logging? * Would you receive an alert/notification if the system stopped logging? * Would there be a loss of records if the audit log gets full? * Are audit records ever overwritten? * How long is audit information retained? * Where is audit retention data located? | *The ISSO may not have been involved but may receive notification if storage fills up.* | * Rules specifying who receives alerts if storage is exceeded |  |
| AU-6 | * How are you involved in the auditing process? * What knowledge do you have of the auditing performed in support of the application or system? | *The ISSO may receive reports reflecting auditing completed. If this is the case, this should be documented in audit procedures. If documented in the procedures that the ISSO receives the reports, but the ISSO does not, that would be a finding.* | * Sample of audit reports provided to the BO or audit records maintained buy the BO |  |
| AU-6 AU-7 | * Describe the process for reviewing logged information. * Is automation used? * Who does the review? * What is reviewed, how often are the reviews performed, and what procedures are in place for documenting the review results? * Who is notified of significant events? * Is a manager-level involved in closure? * Is a weekly, daily, or monthly report generated? * Are patterns looked for in the data? * Is there any aggregation and correlation of events? * How are the events related to the BO and Chief Information Security Officer (CISO)? * Provide information on any tools used to combine audit information from multiple sources, to assist in analysis, or to produce reports that capture the events used for analysis. | *If there is no automated mechanism in place, have the ISSO explain the review process and any correlation between events that might be done. If there is not an automated review, and no correlation of audit data, this may be a finding.* | * Get copy of all events during last 30 days * Get evidence that demonstrates each event was responded to within the established timeframes and closed (email, wet signature, etc.) * Request documentation on the event monitoring process (an event). Once researched, it can turn into an incident and the timeframes for response * Audit review guidelines * Check to ensure each event is rated (low, medium, high) * Look for defined timeframes to research a high event |  |
| AU-8 | * How is time synchronized across internal information systems? | *If there is no time synchronization, this would be finding. Time is critical for forensics when investigating a security incident. It becomes very difficult, if not impossible, when investigating security incidents if the log files on the computers and networks involved contain different references. A time synchronization server should be implemented.* | * Identification of time servers in system inventory/architecture |  |
| AU-9 | * Who has access to audit information (online logs and archived) and audit tools? * How are audit information and audit tools protected from unauthorized personnel? | *Audit information requires additional access controls to prevent intentional or inadvertent modifications of audit records. The information’s integrity is critical when investigating a potential incident.* | * Access control approvals for permissions to view audit records |  |
| SI-1 | * Describe the system and information protection policies and procedures employed to ensure information system integrity. * What mechanisms are in place to look for evidence of information tampering, errors, and omissions? | *The information should be included in the design documentation or SSP.* | * Design documentation * Patch management policies |  |
| SI-2 | * What information does the ISSO receive on security patches? * How do you become aware of patches, hotfixes, and service packs? * How often are patches, hotfixes, and service packs installed? * What is the process (start to finish) from hotfix notification to installation in Production? * How are software hotfixes distributed across systems? * How do you ensure/report that hotfixes have been consistently applied across the environment? | *The ISSO should know about critical security patches and should be included when determining any impact to the system’s security when patches are implemented. The staff that support the system components should also be able to refer to the same patch management procedures, if not, there may need improvement on dissemination of guidance and training if documented procedures exist.* | * Documented procedures for patch management |  |
| SI-3 | * Describe malicious code protections that have been deployed or that you are expecting to be provided (application firewall filters, and Intrusion Detection Systems.) | *The protections identified in the interview should be in line with those documented in the SSP. This could be a lack of documentation or may imply that what is documented is not actually implemented. The Technical Evaluators will be reviewing the rule sets.* | * SSP * Rules (for application firewall filters, IPS, etc.) |  |
| SI-4 | * Describe event/system monitoring performed on the information system. * What tools (Intrusion Detection/Prevention System(s) (IDS/IPS), Security Information and Event Monitoring (SIEM), etc.) and techniques are utilized? * Is event correlation done? * What events are monitored? * Is real-time alerting done if a possible system compromise is detected? | *The protections that are identified in the interview should be in line with those documented in the SSP. This could be a lack of documentation or may imply that what is documented is not actually implemented. The technical evaluators should be reviewing the rule sets for validation/verification.* | * SSP * Rules (for application firewall filters, IPS, etc.) |  |
| SI-5 | * What organizations, besides product vendors, do you receive security alerts from (CSIRC, Security Focus, and US-CERT)? * Who receives these alerts and how is the information disseminated? * Describe the process of what transpires when an alert is received. * How is an alert responded to if it applies to the system? | *Security vulnerabilities can be widespread and receiving notifications from security monitoring organizations can provide insight into solutions.* | * Names of the organizations and mechanism for receiving the information |  |
| IR-1 | * Describe the documented IR procedures. * Are IR personnel identified? * Do the procedures include capabilities for preparation, detection and analysis, containment, eradication, and recovery? * How often are procedures and policies updated? * What is the ISSO’s involvement in the IR capability? | *The ISSO should be a part of the IR capability. Mitigation of incidents depends on a quick and appropriate response.* | * IR guidance |  |
| IR-2 IR-3 | * Describe the IR training personnel receive. * How often is training performed? * After, or in conjunction with, training are periodic IR tests or exercises conducted? If conducted, how often? * Who (individuals or groups) are typically involved? * Are the results and effectiveness/lessons learned reported? | *Quick and efficient response requires an understanding of the steps that must be taken. It is also essential that evidence be handled correctly to preserve the evidence should actions need to be taken so that evidence is not lost or destroyed, which would hamper investigations.* | * Training materials * Evidence of tests or exercise * A list of participants in both |  |
| IR-4 IR-5 IR-7 | * Describe incident-handling procedures that are followed. * To what entity or role does staff report incidents? * How is incident information collected/documented (automated system/database for future correlation)? * Is there a help desk support function where users can report suspected incidents? * Is there a network forensics capability like EnCase Enterprise? * How is the chain of custody insured? * Who performs forensic analysis, if it is necessary? | *The ISSO or another designated security role should be involved in the preservation of the evidence.* | * IR guidance |  |
| IR-6 | * What types of incidents are reported to you? * What is the timeframe in which they are reported? | *Incident-reporting timeframes must be followed—timeframes should be known.* | * Sample of incident reports sent to the BO and possibly email notifications |  |
| IR-6 | * How do you become aware of a security breach or potential breach where the organization claims data was potentially lost or compromised? | *Must follow the organization’s incident reporting process and understand their responsibility should an incident occur.* | * IR procedures noting the notification process and the process for notifying the business owner. |  |
| AT-1 | * Describe security awareness training policies and procedures. * What is your role in ensuring that all staff receives awareness training? |  |  |  |
| AT-2 AT-3 | * What types of security awareness and role-specific training have you attended? * Have you attended any vendor or additional training (beyond corporate security awareness training) where the focus is on information/data security? | *The ISSO should have a key role in ensuring that all staff has the appropriate training, whether it is for awareness or role-based training. All staff supporting system components must understand the implications of insecure implementations of the component. They must also ensure that configurations are set to the most restrictive setting possible. To do this, they must have an understanding on what the settings are and how to implement them appropriately.* | * Training materials and position descriptions with security training requirements |  |
| PM-15 | * What professional groups are you and the organization associated with that provide information and dialogue concerning current security practices? | *Being involved in professional organizations provides a means to stay current on security issues and solutions. This is an inexpensive means when training or security staff is limited.* | * List of organizations staff are associated |  |
| CA-2 CA-7 | * What methods are used to ensure security controls are implemented correctly and operating as intended? * How often is that done? * If recertified, do you have previous system certification? | *This assessment is one of the mechanisms for compliance; however, the BO has the role of ensuring continuous monitoring activities, including CM and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting.* | * Samples of previous assessments, reports, and monitoring reports received |  |
| CA-3 | * Are there information systems outside the accreditation boundary the system connects to? * What is the process to obtain authorization for a connection? | *The BO ultimately is responsible for ensuring that all these connections are documented in the SSP and Information System Risk Analysis (ISRA).* | * Samples of interconnection agreements |  |
| CA-5 | * What Plans of Action and Milestones (POA&M) items were identified from the previous assessment? * Do any POA&M items remain open? * What is the process for closing POA&Ms after the security assessment is completed? * How do you validate that a POA&M can be closed? | *There should not be simply an implicit trust that if the vendor claims a finding is fixed that this is accepted. The evaluation criteria should include that the BO must demonstrate that they seek subject matter expert (SME) consulting when closing out POAMs. Thus, there should not be only a direct question, but rather a series of questions where the BO is given every opportunity to state that they get any applicable stakeholders involved. If they never do, then this is a finding.* | * POA&Ms from prior assessment(s) |  |
| CA-6 | * When was the system accredited? * If the system was previously accredited, do you have supporting documentation from the organization’s controls tracking system? | *System should have been accredited prior to being placed in production.* | * Authorization package documentation and any applicable supporting documentation |  |
| RA-1 | * Describe RA policies and procedures. | *A few questions need to be asked; however, most information will be obtained from the RA review.* | * RA and other assessments |  |
| RA-2 | * What was the process for categorizing the system? | *The ISSO should be an advisor to the BO for this process and may actually have performed the categorization on the BO’s behalf. The categorization is critical as selected controls rely on the categorization. Verify the level for example: The organization has selected a moderate categorization for most systems that contain PII. The GSSs are generally considered high.* | * Categorization documentation, if not included in the SSP |  |
| RA-2 | * How frequently are RAs performed? * How are you involved in risk-based decisions? * What constitutes a significant change that would prompt a RA? * Describe the RA approval process. * Does senior management sign-off (approve) RA results? | *The BO must accept any remedial risks and has the responsibility to mitigate those risks. Risks are identified if the system has not implemented required security controls. For all identified risks, there must be a POA&M.* | * Waivers for acceptance of risks and POA&Ms for identified risks |  |
| RA-5 | * What process is in place and documented that monitors new vulnerabilities for each footprint in the environment (operating system, databases, network devices, etc.)? * Does the organization subscribe to a vulnerability service? If yes, get a description. * How frequently is the system scanned for vulnerabilities? * What tools are used? * Who receives scan reports/outcome? * Are the personnel who run the tools trained in how to use them? * If patches are required, how quickly can patching be performed? | *All the information should be in the SSP; however, the ISSO should also have knowledge of these processes.* | * Reports or outcome from scans that are sent to the ISSO/BO |  |
| SA-2 | * How was security planned for during the IT investment process to ensure that the information system was adequately protected? | *The BO must allocate adequate funding during the investment process to implement the required controls.* | * System Software Development Life Cycle (SDLC) and design documents addressing security controls |  |
| SA-4 SA-9 | * How are security requirements and/or security specifications included in information system acquisition contracts, either explicitly or by reference? * What are the requirements? * Are there security requirements for external providers for the system that might be placed in contracts or service agreements? | *The ISSO may advise the BO on the inclusion of security requirements in information system contracts. The organization has standard clauses to be included. Sometimes, contracts are not reviewed by the Office of Information Services (OIS).* | * Systems contracts and service level agreements (SLA) |  |
| SA-5 | * Who maintains documentation associated with the information system (documentation that describes the system and purpose, technical operation, access controls, maintenance, and required training for administrators and users)? | *The ISSO has some responsibility to ensure that all required documentation for the system is developed and maintained per the organization’s guidance.* | * List of all documentation, if not in the SSP |  |
| SA-6 | * How does the organization ensure adherence to software license restrictions? * Are end-user workstations and laptops periodically scanned for unapproved software? * Is a software license inventory maintained? * Does the ISSO have any role to ensure restrictions are adhered? | *The ISSO may have responsibilities associated with adherence to the software restrictions, random audits, etc.* | * Software licenses and policies associated with software licenses |  |
| CM-11  SI-7 | * What software are users permitted to install on their workstations and laptops? * What guidance has been provided to users regarding the types of permitted software installations (updates and security patches to existing software) and what types of installations are prohibited (free software only for personal, not government, use, as well as software whose pedigree with regard to being potentially malicious is unknown or suspect). | *The ISSO may be responsible for disseminating the information.* | * Guidance associated with maintaining workstations |  |
| SA-10 SA-1 | * How is CM handled during the development process to ensure proper testing of controls? * Do you review the developer’s Configuration Management Plan (CMP) that controls change during development, tracks security flaws, requires authorization of changes, and provides the plan’s documentation and its implementation? * Are developers required to create a Security Test and Evaluation Plan, implement the plan, and document the results for system changes? * Is PII used to test the system in the development region? * What situations warrant a plan? * Was that plan approved? * Was it approved prior to testing? | *The ISSO should review the process for controlling the system during development to ensure that the controls as designed are implemented and appropriately tested during the development process.* | * Developers security checklist for testing and ensuring controls are adequately tested |  |
| CM-1 | * What are the documented CM procedures? * Are there documented timelines that ensure each “rated” vulnerability is tested and implemented within the defined timeframes? For example, if Microsoft issues a critical patch or hotfix, how would the vendor react? * Is the organization involved in the process? * Is there an emergency change management process? * If patches are made directly in the Production Environment, how do vendors ensure that unauthorized changes are not also made? * Who has oversight for CM processes? | *For changes directly in Production, the organization BOs need to approve and accept risk.* | * CM guidance that addressed all components in the environment (operating system, databases, network devices, etc.) |  |
| CM-2 CM-6 | * How are baseline configurations developed and documented? * What tool is used to ensure that the approved baselines remain the implemented baselines? * How often is the baseline updated? * What triggers the update process? * What is the process? * What was used to determine how to set security configuration parameters or determine the services needed? | *The vendor should periodically (weekly) check to ensure that the approved baselines are still intact.* | * Baseline configurations that are validated against the implemented configurations, records of updates to the configurations, and records of configuration scans and comparison against the production-implemented configurations |  |
| CM-3 | * What is your involvement in the process that controls change to the information system? * Is there a Change Control Board (CCB)? * If so, do you participate in CCB board activities? * How are changes authorized in the environment? * What is the process to implement emergency changes? * How is security addressed by the board or who represents the security interests related to the change? * What is the business exposure if there is a system outage? | *Proper CM and change control prevent system outages and mitigate the business exposure. The BO or its organization, which includes the ISSO, should ensure that the system has all required documentation, and that the documentation is updated as changes are made. Change Requests (CR) will be approved by the BO or the BO’s designated representative and other appropriate organization officials, including but not limited to, the system maintainer and information system support staff* | * CM documentation * Change records noting the approval process with signatures * CCB documentation * Examples of approved changes |  |
| CM-3 | * What is the process to test, validate, and document changes (patches and updates) before implementing the changes in the Production Environment? * What reports are generated? * How would you know if a change was made in the Production Environment? * Is a host-based IDS used? * How are the change management process and “detection” process integrated? * How are security controls confirmed to ensure they still function properly after changes have been deployed? * Do you test after the change was made in the Production Environment? | *Does the ISSO review all changes to the Production Environment, does the ISSO validate against the change control documentation to ensure only approved changes are implemented. Assuming the vendor can detect a change in the production environment, and then the next step would be to determine if there was a planned change expected via the change management process. For example, if a router IOS or firewall was upgraded, then the implemented change should be tested.* | * Records of approved changes to compare against implemented changes |  |
| CM-8 | * What is the process to maintain the inventory of information systems and their components? * Is there an approved inventory (asset) list? * Is there a tool that periodically revalidates the approved environment? * Is there an automated mechanism to help maintain an up-to-date, complete, accurate, and readily available inventory of information systems and their components? | *Who has the ultimate responsibility for maintaining this inventory?* | * Records |  |
| MA-1 MA-2 | * What are the policies and procedures associated with maintenance of the system and its components? * Explain MA activities to include routine, scheduled maintenance, and repairs, whether performed onsite or remotely, and whether the equipment is serviced onsite or removed to another location. | *MA activities are required to ensure system availability.* | * Records of maintenance |  |
| MA-2 MA-5 | * What type of records are maintained (i) date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of the escort, if necessary; (iv) description of maintenance performed; and (v) list of equipment removed or replaced (including identification numbers, if applicable)? * Is there a list of personnel authorized to perform maintenance on the information systems? * Who has access to the list? * How are MA personnel verified? * Request to see the list. | *If no MA log is kept and the above information is not recorded, this would be a finding. The ISSO may not maintain the log; however, the ISSO should review the log to ensure that they are appropriately kept.* | * List of authorized MA personnel * Review MA logs |  |
| MA-2 MA-3 | * What agreements or arrangements are in place regarding diagnostic equipment and software that vendors may bring onsite? * How is it monitored? * Are you aware of how access to tools is restricted to MA personnel? | *The ISSO should have knowledge of the tools being used and restrictions enforced.* | * Any agreements or prior approvals for equipment to be brought in for diagnostic * Authorization to bring/take equipment from facility |  |
| MA-4 | * What ability do the vendors have to perform remote diagnostics and maintenance? * How is remote diagnostics and maintenance authorized, monitored, and controlled? * Are records for remote maintenance maintained? | *Remote maintenance should be documented in the SSP and the ISSO should have knowledge of the tools being used and restrictions enforced.* | * Request maintenance records |  |
| MA-6 | * Describe the SLAs with MA vendors (turn-around time). * Are any spare parts stored onsite? * Where are spare parts located onsite? * Is there a documented MA schedule? | *SLAs should be documented in the SSP.* | * Maintenance schedule |  |
| SC-1 | * Describe the system and communication protection policies and procedures employed to ensure the information system’s integrity. | *A few questions need to be asked since most of the control satisfaction will be determined via testing. These questions are also asked of the SysAdmins in case they are responsible for key management.* | * MA Schedule |  |
| SC-12 | * If cryptography is required and used within the information system, describe the process for managing cryptographic key generation, distribution, storage, use, and destruction. * Is the process documented? | *The ISSO should have documented all uses of cryptography and the management of the keys as it pertains to the information system. The system may be dependent on the GSS for these services, but this should be clear in the SSP.* | * Key management procedures |  |
| CP-2 | * What is your involvement in planning the recovery of the application/system? * What has been your involvement in component recovery prioritization? * What has been your involvement in testing the plan? | *The BO should be involved in the recovery process. If the system is one that is used to provide a service to the organization and the only users are internal, the BO’s involvement may only be notification. The BO, if an end user, should be familiar with testing and approval of the recovered system.* | * Business owner being identified in the Contingency Plan |  |
| CP-2 | * Describe any business impact analysis performed for the system. * What is the required Recovery Point Objective (RPO) for the system (describes the acceptable amount of data loss measured in time) and the Recovery Time Objective (RTO) (how soon does it need to be made available if a recovery needs to be performed)? | *The RPO and RTO must be considered when determining the method for recovery of the system. The BO should still be involved in the Business Impact Analysis (BIA). If the system is one that is used to provide a service to the organization, and the only users are internal, the involvement of the BO may be minimal in RPO and RTO planning.* | * BIA |  |

# Human Resources (HR) / Personnel Security

The system stakeholders should provide an overview of their roles and responsibilities related to the application or system, as well as the controls in place to secure it. The overview should include all components for which they have a specific responsibility to ensure security in relation to the application or system.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control(s) | Question(s) | Guidance | Evidence Examples | Response |
| PS-1 | * Describe the Personnel Security policies. * Describe the purpose, scope, roles, and responsibilities of the policy. * How is alignment with the organization’s PS requirements or contract requirements ensured? | *There should be written procedures describing details of how policy requirements and screening criteria are met for the system being evaluated in terms of who initiates/authorizes the PS clearance process for this system’s users, which forms need to be filled out, where is it routed and what other requirements need to be met before the user is granted access to the organization’s system and/or the data.* | * System-specific PS procedures or SSP addressing personnel screening criteria * Examine records of screened personnel and other relevant documents or records |  |
| PS-2 | * How are sensitivity ratings (non-sensitive, public trust, etc.) assigned to positions? * What are the sensitivity ratings for the staff supporting the organization’s systems? Provide the supporting information. * How often are they reviewed? | *There should a written procedure describing how the security clearance level is reviewed and the review’s frequency to determine continuous need.* | * Records of periodic rescreening individuals accessing the system to determine the position’s sensitivity rating |  |
| PS-3 | * Describe the screening process performed prior to system access for potential employees. * How is IT notified when staff have been screened as required and can be provided system access? | *Documented procedures should be available for employee screening process.* | * Ensure that the organization’s personnel screening procedure is followed |  |
| PS-4 | * How does the termination process work —amenable and non-amenable (i.e., emergency termination process)? * What is the process for revoking access if an employee is terminated or resigns? What is the time frame? Is it immediate? * Is all system property immediately collected and who is responsible? * Is there an exit interview and who performs it? | *For termination the revocation should be immediate. Documented user termination procedures should be available describing timeliness in revoking system access, as well as physical access rights. Written procedures should include a process for conducting exit interviews; collecting keys, ID cards, and building passes; retrieving system-related property from the terminated user; and ensuring that the authorized person can retain access to the official documentation created by the terminated user. For privileged users, access rights should be removed prior to contact with the employee. Is this documented?* | * Documented record of terminated employee showing the process was communicated throughout the commendation channel |  |
| PS-5 | * Describe employee transfer procedures. * Is system access reviewed? * Are old accounts closed and new accounts opened? * Are keys (i.e., physical/logical) and building passes collected? | *Documented employee transfer procedures should be available describing how old accounts and access privileges are terminated and new accounts are created, including a process for reviewing appropriate security clearance level and reissuing ID cards and building passes.* | * Documented record of transferred employee showing the employees’ access was terminated from the current position and the procedure for granting/establishing access for new position |  |
| PS-6 | * What are employees required to sign prior to system access (i.e. access agreement, Rules of Behavior (RoB))? * Are access agreements reviewed, if so by whom? * Where are they kept and for how long? | *Determine if system access requires a signed agreement before system access is authorized to users. Verify if such records are maintained by the System Owner (or the authorized officials).* | * Sample of RoB and other relevant agreements signed by system users |  |
| PS-7 | * What PS policy and procedures are third-party providers (i.e., contractors) subject to? * What is the process for contractor access to IT systems? | *If the system allows physical and/or logical access to third-party providers, then there should be documented procedures describing how third-party access is authorized/approved, what level of access is allowed, third-party roles, and the requirements for appropriate access agreements to be signed and maintained by both sides.* | * List of PS requirements for third-party providers, such as vendors, contractors, etc. * Examine third-party compliance monitoring records, if available |  |
| PS-8 | * How are personnel handled if they violate PS policy or procedures? * Is the process formally documented and are employees aware of the process? | *System users should be aware of the appropriate penalty and sections for any violation of the organization’s policy.* | * Provide the policy noting violation ramifications |  |

# <Other Role(s) (As Needed)>

The system stakeholders should provide an overview of their roles and responsibilities related to the application or system, as well as the controls in place to secure it. The overview should include all components for which they have a specific responsibility to ensure security in relation to the application or system.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control(s) | Question(s) | Guidance | Evidence Examples | Response |
| All “-1” Controls |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |