

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>)

Network and/or Operating Systems  
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 Details

Table . Interview Logistics

|  |  |
| --- | --- |
| Date of Interview |  |
| Location of Interview |  |

Table . Interviewer(s)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Role | Name | Organization | Phone Number | Email Address |
| Interviewer |  | Assessment Team |  |  |

Table . Interview Participants

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Role | Name | Organization | Phone Number | Email Address |
| Assessment POC |  |  |  |  |
| 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. Access Control and Identification and Authentication 1](#_Toc199483513)

[2. Audit and Accountability 7](#_Toc199483514)

[3. System and Information Integrity 12](#_Toc199483515)

[4. Incident Response 15](#_Toc199483516)

[5. Awareness and Training 17](#_Toc199483517)

[6. Risk Assessment 18](#_Toc199483518)

[7. Configuration Management 19](#_Toc199483519)

[8. Maintenance 21](#_Toc199483520)

[9. Contingency Planning 23](#_Toc199483521)

[10. Media Protection 26](#_Toc199483522)

[11. System and Communications Protection 28](#_Toc199483523)

# 

# Access Control and Identification and Authentication

Access Control ensures only authorized users, processes, or devices can access information systems and resources.

Identification and Authentication verifies the identity of users, processes, or devices before granting access to systems.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control(s) | Question(s) | Guidance | Evidence Examples | Response |
| AC-1 AC-2 | * What responsibilities do you have for establishing AC for the system or environment or system components you support? * Describe the process for establishing and activating accounts. * Describe the process for modifying access (only applicable if there are multiple roles associated with the application (e.g., What is the process for someone with read-only access that now has a need for update access).) * Describe the process for disabling and removing accounts (e.g., if an employee quits, how is the account removed from the application/system?).) * What is the process for disabling and removing accounts associated with emergency terminations, in particular for “SUPERUSERS” (aka privileged users)? * When there is a termination, is access removed prior to the employee being notified they are being laid off or otherwise terminated? * Are accounts deleted if not what is the reason they are retained? (e.g. historical purposes?) | *Formally documented system-specific account management procedures should be in place. A procedure may be in place but may not be followed. These procedures should include steps for granting and terminating system access, the system’s audit capacity to support tracking and monitoring user activities, and the frequency of periodic review process. If the interviewee has no privileges associated with account management, then many of the follow-up questions may not be necessary. The procedures should be validated through information gathered by the Technical Evaluator through the last logged in dates (exceeds inactivation requirement). The formally documented record for each account that is created, modified, and recertified should be available for review.* | * Formally documented procedures associated with system-specific account management, access request forms, workflow with authorized approver lists, and defined list of user roles * Sample document with signature of authorized person approving user access to this system * List of active users and system-generated record of User IDs with last login time and date * Lists of recently transferred, separated, or terminated employees with transfer/termination dates and 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 * Collection of evidence where the BO has “signed off” on yearly access (both ID and roles/privilege) |  |
| AC-2 | * How often are accounts reviewed to determine if access is still needed by the user? * What are the escalation procedures if there is an issue? * How are inactive accounts handled? (e.g. disabled after a period of inactivity, length of time that they remain active in the various components) * Are automated audit mechanisms employed to record this activity? | *From a security perspective, expect the Information Technology (IT) department to periodically produce a list of users and their privileges/roles and present this list to the approving authority for reaffirmation. The frequency of periodic reviews of regular and privileged user accounts should be established. Management should track and monitor privileged role assignments more frequently as required by the organization’s policy. The use of privileged accounts and administrative function should be strictly controlled. The period should be at least once every year for a “typical”’ user, but more frequently for privileged users. This frequency for privileged users may range from 30 days, where there are a large number of privileged users since chances are that someone can get “lost” in the crowd, versus every quarter where there is a tight-knit user community.* | * List of accounts for certification/validation * Record of periodic review of regular user accounts * Record of periodic review of privileged user accounts * Review automated account policy settings disabling the inactive user account |  |
| AC-2 IA-4 | * Describe the use of temporary and/or default system (or service) accounts. * If used during an operating system or an application is installation, when are they removed? | *Temporary accounts should be removed. If this is done, it will be evident when Technical Evaluators’ reviews are complete. If default system accounts (or service accounts) are required for system operation, then they should be changed immediately and managed with strict password policy. Otherwise, they should be disabled.* | * Verified by the Technical Evaluator from technical script output |  |
| AC-5 | * How is separation of duties enforced? * Describe the use of groups/roles. How are users assigned? * What privileges are granted to administrators? * How does the account management process ensure that employees are given the least amount of system privileges to perform assigned duties? | *The separation of duties should be implemented by ensuring that certain roles are separated and divided among different individuals to prevent conspiracy for malicious activities. For example, the Minimum System Security Officer’s (performs audit functions) and the System Administrator’s (SysAdmin) roles (implementing AC and performing other administrative functions) should be separated in the Production Environment. The Developer or Evaluators should not have access to any data or configuration files in the Production Environment.* | * System-specific documented account management procedures * Review and compare the user access list to see if the same users have access to multiple conflicting roles in the same environment or the same user has same role in the multiple environments |  |
| AC-17 AC-20 IA-2 | * What remote access to system components is permitted? * What is the process to obtain authorization for remote access? * How is AC enforced for remote access? * How are remote users identified and authenticated? * Is multifactor authentication used? * Is cryptography used to protect remote access sessions? * Are there a limited number of remote AC points? * Who is authorized to remotely access the systems? * How is access monitored? * Is there an automated audit capability to log the activities associated with remote access? * What guidance is provided to personnel working from home (e.g., fundamental security controls and practices that include passwords, virus protection, and personal firewalls)? | *An Administrator may grant access. Remote access for privileged functions shall be permitted ONLY for compelling operational needs and it must be APPROVED IN WRITING BY THE Chief Information Officer (CIO) or CIO’s designated representative. Dial-up lines, other than those with FIPS 140 (as amended) validated cryptography, SHALL 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 * System-specific formally documented remote access procedures, if applicable |  |
| AC-18 | * How is wireless access used? * How is wireless access controlled? * How is wireless access protected? * Do you scan for unauthorized wireless access points? | *Administrator may use support wireless access. If allowed, it should be limited. Wireless access is prohibited unless APPROVED IN WRITING BY THE CIO or CIO’s designated representative. If approved, the organization’s Minimum Security Requirements (MSR) have strict guidance on technical controls that must be in place. Check with Technical Evaluators.* | * Approvals from the CIO * Access forms for wireless access demonstrating approval process * System-specific formally documented wireless access procedures, if applicable |  |
| AC-19 | * What use of personal computers/devices to access the system by authorized users is allowed? * If allowed, what role do you have in securing these devices? * What infrastructure is in place to support secure use of these devices? | *The implications to the assessor (if answer is “yes”) is to ensure that the technical infrastructure is in place to support the use of “unknown secure computers” into 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 play a bigger role is where a SysAdmin gains access thru the ‘backdoor’ to manage the systems during off hours/weekends, etc. (a typical scenario). In this case, if an untrusted asset is allowed system access without controls, then there is a Finding. What constitutes effective controls for this backdoor access? Answer: usage of a Citrix server properly configured.* | * Approvals from the CIO * Access forms for the use of personal computers/devices demonstrating the approval process |  |
| AC-20 | * What access is allowed using external information systems (including outsourced systems)? * If allowed, what role do you have in securing these devices? * What infrastructure is in place to support secure use of these devices? | *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 System Security Plan (SSP) * Connection agreement documents, if applicable |  |
| IA-2 | * How are users uniquely identified and authenticated? * How is multi-factor authentication requirement implemented for this information system for privileged and non-privileged accounts? * What are the two factors of authentication that are used to access the system? * What certificates are used? * Are group accounts used? * If group accounts are used, which group accounts are used and for what purpose? * What are the process highlights to gain management approval? | *If group accounts are used, this should be identified in the SSP and have limited use. Its use must be controlled and monitored closely. For multi-factor authentication reference IA-2(1).* | * Approval for use of group accounts, if used |  |
| 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)? | *Have the administrator explain why they are used and how they are secured.* | * Approval process for devices that requires IA |  |

# Audit and Accountability

Audit and Accountability enables the recording, examination, and accountability of system activities to detect and respond to security incidents.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control(s) | Question(s) | Guidance | Evidence Examples | Response |
| AU-1 | * Explain all auditing performed in support of the operating system or component that you support, including the responsibilities associated with capturing all data, reviewing records, and the 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 general support system (GSS) components. * What information is gathered? | *System-specific audit procedures should be established describing audit roles and responsibilities, events to be audited and appropriate contents to be logged to support after the fact investigation. Audit logs should not be able to be modified or deleted. Users (whether regular or privileged users) whose activities are logged in the audit logs should not be able to alter the audit logs in any way. Ideally, the audit records are reviewed by staff that does not have administrative responsibilities for the system component that created the audit record.* | * System-specific formally documented audit logging and monitoring procedures * Request sample audit reports that are produced |  |
| AU-2 AU-3 | * How are generated audit 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, and hardware/software element) for each event record? * How is the correlation between events and users performed? | *ISSO (or person with system security responsibilities) should ensure that important events are logged (e.g., successful/unsuccessful logon attempt, access modification, user activities of file level changes, system startup/shutdown, system errors, command line or batch file changes, audit capability turned off) with sufficient details (e.g., date/time, type of event, user/subject, success/failure, and hardware/software element) to support after-the-fact investigation pertaining to this system. The content of the audit records may be reviewed by Technical Evaluators. These interview questions should validate the ISSO’s knowledge and the ISSO’s involvement O 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. Where possible, there should be automated mechanism in place to correlate audit data from various audit logs to determine the appropriate level of risk.* | * Request samples of audit records from Production Environment to see what events are being logged and how many details are logged for each event * If possible, obtain records produced by the Application Evaluator. Usually this is not possible since testing is not generally done in the Production Environment and many audit records are not logged into the other environments |  |
| AU-4 AU-5 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 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 got full? * Are audit records ever overwritten? * How long is audit information retained? * Where is audit retention data located? | *There should be system-specific audit storage capacity defined. Automated setting should be configured to support appropriate audit storage capacity. Audit records should be archived before older events are overwritten. The ISSO or person with system-specific security responsibility should be able to demonstrate what the mechanisms in place are to alert/notification if the system stopped audit logging. The administrator should be involved in the storage requirements and should receive notification if audit logging failed or it would be a finding.* | * System-specific audit procedures showing the audit storage capacity and frequency of audit logs archiving * Formally documented procedures specifying who receives alerts if storage is exceeded and/or system stopped audit logging |  |
| 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 review results? * Are ACs (i.e., accounts, access to directories/files) reviewed to ensure they are working/set as intended? * What is the process, who performs the review, and how often is the review performed? * How often are administrator level groups and level accounts reviewed? * What is the review frequency of regular user activities? * What is the review frequency of privileged user activities? * Who is notified of suspicious activity or significant events? * Is a Manager level involved in closure? * Is a weekly, daily, and/or monthly report generated? * Are patterns looked for in the data? * Are any aggregation and correlation of events performed? * 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, assist in analysis, produce reports that capture the events, and are used for analysis. | *There should be system-specific formally documented review procedures describing roles and responsibilities and the frequency of various audit records. If there is no automated mechanism in place, have the ISSO explain the review process and any correlation between events that might be done. A periodic review of user activity logs and frequency of review should be established. If there is no automated review and no correlation of audit data, this may be a finding. Account review should be incorporated in audit procedures—confirms that is the practice. Administrator accounts must be reviewed by staff not responsible for the specific component. These reviews must be done more often with Moderate requirements. They must state administrator groups, root accounts, and other system-related accounts and must be reviewed on demand, but at least once every fourteen (14) days. This may be included in the audit review process.* | * System-specific documented review procedures * Evidence showing established audit procedures are followed * Evidence of periodic review of user activities (regular users as well as administrator users) * Copy of all events during the last 30 days * Evidence that demonstrates each event was responded to within the established timeframes and closed (i.e. email, wet signature, etc>) * Documentation on the event monitoring process (i.e. an event, once researched, can turn into an incident and the timeframes for response) * Audit review Guidelines * Check to ensure each event is rated (low, medium, high) and look for defined timeframes to research a high event? |  |
| AU-8 | * How is time synchronization across internal information systems done? | *If there is no time synchronization, this would be a 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 time references. The system’s (and all the components within the system’s boundary) internal clock should be regularly synchronized with the central time server.* | * System-specific procedures addressing time stamp procedures * Examine various logs to see if the time stamps are synchronized within different logs |  |
| AU-9 | * Who has access to audit information (i.e., online logs and archived data) and audit tools? * How are audit information and audit tools protected from unauthorized personnel? | *Audit information requires strict access control to prevent either an intentional or inadvertent modification of audit records. The integrity of the information is critical when investigating a potential incident.* | * Access control approvals for permissions to view audit records * Review who has what type of access to audit records |  |
| AU-11 | * How long is audit information retained? * Where is the audit retention data located? | *The administrator will have a role in the audit retention and backup data location. Audit records should be retained at least for one year. Audit information requires additional access control to prevent either an intentional or inadvertent modification of audit records. The integrity of the information is critical when investigating a potential incident.* | * Ask for audit records as old as 365 days |  |

# System and Information Integrity

System and Information Integrity detects and responds to flaws, vulnerabilities, and unauthorized changes to maintain system integrity.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control(s) | Question(s) | Guidance | Evidence Examples | Response |
| SI-1 | * What mechanisms are in place to look for evidence of information tampering, errors, and omissions? * Who would be alerted? | *The information should be included in the design documentation or SSP* | * Rules for the tools or mechanisms in place |  |
| SI-2 | * How do you identify flaws within the system? * Do you have a formal procedure to report identified flaws? * What details are recorded in the report? * Are flaw remediation procedures identified (and integrated) within the system-specific configuration management process? * How do you become aware of patches, hot fixes, and service packs to remediate system flaws? * How often are patches, hot fixes, and service packs tested and installed? * What is the process (start to finish) from flaw remediation notification to installation in the Production Environment? * How are software fixes distributed across systems? * How do you ensure/report that fixes have been consistently applied across the environment? | *System-specific documented flaw identification and remediation procedures should be available for review. The ISSO (or the person with system-specific security responsibilities) should monitor the flaw remediation activates, including testing and installing critical patches and fixes in a timely manner. Procedures should be in place to determine any impact to the system’s security when flaw remediation measures (i.e., patches, hot fixes, etc.) are implemented. The staff that supports system components should also be able to refer to configuration change control and patch management procedures.* | * Documented procedures for flaw remediation (i.e. patch management, etc.) * Evidence that the system-specific CM process includes flaw remediation procedures with appropriate details * Flaw remediation related audit logs |  |
| SI-3 | * Describe malicious code protections deployed on your system. * What type of malicious code protection mechanisms are implemented: * How often are signatures updated? * What type of scanning is performed? * How often is scanning performed? * Who reviews scan results? | *System-specific malicious code protection requirements should be defined in the SSP, describing how these requirements are met within all the system’s operational components. Automated audit logs should be generated to track signature updates and scanning history* | * Review system-specific malicious code protection procedures * Audit log sample showing regular updates of the signature files on all the system components * Vulnerability scanning results * CM document describing configuration settings requirements of virus scans (or any other malicious code protection software installed) |  |
| SI-4 | * How is IDS/IPS deployed on your system components? * Is IDS host-based, or network-based, or both? * Describe the event/system monitoring performed on the information system. What tools (IDS, IPS, and SIEM) and techniques are utilized? * Is event correlation performed? * What events are monitored? * Does IDS provide near real-time analysis of events? * Does IDS send out real-time alerts or notifications to appropriate individuals? * What is the procedure for responding when a compromise is detected? | *There should be automated mechanism implemented to support intrusion detection/prevention. The organization’s policy requires that all systems are protected with automated IDS/IPS mechanisms. Where applicable, SSP should document the mechanisms used to monitor information system integrity.* | * System Design Document addressing information system monitoring tools and techniques used * CM document describing configuration settings, services, and protocol requirements of system monitoring tools |  |
| SI-5 | * Which organizations, outside of product vendors, do you receive security alerts from? * Who receives these alerts and how is the information disseminated? * Describe the process of what transpires when an alert is received. If an alert applies to the system, who responses to it? Who is their back-up? | *Staff with system security responsibilities should keep up-to-date with current security alerts and advisories that affect the system and maintain situational awareness of the threat posing their system. There should be procedures in place to disseminate security alerts, advisories, and directives to identified individuals so they can take appropriate action, in timely manner, to protect the system components and its operation.* | * Records of security alerts and advisories received and disseminated to identify individuals |  |
| SI-8 | * Describe how spam protection is implemented. | *Automated mechanism should be implemented to detect and take action on unsolicited messages transported by email, email attachments, Web access, removable media, or other common means.* | * System Design Document addressing spam protection tools and techniques used * CM document describing configuration setting, spam protection software, and tools |  |

# Incident Response

Incident Response provides a structured approach to detecting, reporting, analyzing, and responding to cybersecurity incidents.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control(s) | Question(s) | Guidance | Evidence Examples | Response |
| IR-1 | * Describe the IR procedures. * Do the procedures include capabilities for preparation, detection and analysis, containment, eradication, and recovery? * How often are procedures and policies updated? | *The organization’s IR policy should be followed. Appropriate procedures should be developed at the system level to support the organization’s IR policy. Incident Response capability planning activities should be coordinated between System Owner, ISSO, BO, and other relevant individuals supporting the system.* | * The organization’s Incident Response policy and guidance * System-specific IR procedures, if applicable |  |
| IR-2 | * Describe IR training personnel receive. * Are IR personnel identified? * How often is training performed? * What are your IR responsibilities? | *A 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 the appropriate chain of custody maintained so that evidence is not lost, contaminated, or destroyed during the handling of the incident, which would hamper investigations. SSP should reference IR training frequency.* | * IR training materials * Record of periodic training received by involved individuals * Evidence of tests or exercise * List of individuals who participated in training |  |
| IR-3 | * How are IR tests and exercises conducted? * If IR tests and exercises are conducted periodically, how often? * Who (individuals or groups) is typically involved? * Are results and effectiveness/lessons learned reported? | *IR training must be repeated at least once a year.* | * Evidence of periodic IR tests or exercise * List of participants |  |
| 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 that users can report suspected incidents? * Is there a network forensics capability, like EnCase Enterprise? | *SSP should document the system-specific procedures for reporting an incident.* | * SSP or system-specific IR process |  |

# Awareness and Training

Awareness and Training promotes security awareness and provides necessary training to ensure users understand and follow security responsibilities.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control(s) | Question(s) | Guidance | Evidence Examples | Response |
| AT-2 | * What security awareness training (i.e., annual security awareness training) have you attended? | *There should be procedures in place to provide security awareness training as part of initial training for new users. This training should be held prior to granting system access and then repeated every 365 days thereafter.* | * Review users training records |  |
| AT-3 | * What vendor or additional training (beyond Corporate Security Awareness Training) with the focus on information/data security have you attended? | *In addition to basic awareness training, specific role-based training should be provided (e.g., Security training for Windows or UNIX administrator, Network administrator, database administrator, application developer, system administrator).* | * Record of specific role-based training addressing security implication within the areas of individual subject matter expertise |  |
| PM-15 | * What professional groups are you associated with that provide you with information and dialogue concerning current security practices? | *Depending on the operation and system sensitivity, there may be system-specific requirements for additional external training (CISCO Firewall administrator training or Medicare data handling training).* | * Review requirements for maintaining external training * Record of such training, if applicable |  |

# Risk Assessment

Risk Assessment identifies, evaluates, and prioritizes risks to inform security decisions and risk response strategies.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control(s) | Question(s) | Guidance | Evidence Examples | Response |
| RA-5 | * How frequently is the system scanned for vulnerabilities? * What tools are used? * Who receives scan reports/outcome? * Is the staff who run tools trained how to use them? * If patches are required, how quickly can patching be performed? | *A few questions need to be asked, although most information will be obtained from the RA review.* | * Reports or outcomes from vulnerability scanning performed on all system components, as applicable (For the comprehensive assessment scan results from network devices as well as servers, workstations, etc.) |  |

# Configuration Management

Configuration Management maintains system integrity through secure configuration settings, change control, and baseline management.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control(s) | Question(s) | Guidance | Evidence Examples | Response |
| CM-1 | * Describe the documented CM procedures. * Examine the procedures for add and updating the configurations. Are there areas that the documented policy does not address, such as testing the new configuration, updating the Version description document or baseline configurations? | *The organization’s CM policy should be followed.* | * System-specific formally documented CM procedures |  |
| CM-2 CM-6 | * How are the baseline configurations developed and documented? * How often is the baseline updated? * Who updates the baselines? * What triggers the update process? * What is the update process? * What was used to determine how to set security configuration parameters or determine the services needed? | *The security configuration baseline should be determined and locked for all system components. The vendor should periodically (weekly) check to ensure the approved baselines are still intact.* | * Baseline configurations that are validated against the implemented configurations * Records of updates to the configurations * Records of configuration scans and comparison against the production implemented configurations |  |
| CM-3 | * What is the approved process for authorizing, documenting, and controlling changes to the information system? * Is there a Change Control Board (CCB)? * How are changes authorized in the environment? * What is the process to implement emergency changes? * Is there a process to test, validate, and document changes (patches and updates) before implementing the changes in the Production Environment? * How are security controls confirmed to ensure they are still functioning properly after changes have been deployed? * What reports are generated? | *The SysAdmin should work with the ISSO or BO to ensure that only necessary, authorized, and tested changes are implemented in the Production Environment. System-specific validation and testing processes should be documented.* | * 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 automated mechanism to help maintain a current, complete, accurate, and readily available inventory of information systems and their components? | *A hardware/software inventory should be documented in the SSP.* | * SSP and other system-specific records |  |

# Maintenance

Maintenance ensures that systems are properly and securely maintained to preserve functionality and security posture.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control(s) | Question(s) | Guidance | Evidence Examples | Response |
| MA-1 | * Describe the documented MA procedures. * Examine procedures. Do they address everything in the MA policy? | *System-specific MA procedures should be developed as required by the organization’s policy.* | * System-specific policy, procedures, and supporting documents |  |
| MA-2 | * 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. | *This is a system-specific control. System-specific maintenance requirements and the procedures should be documented, describing one- time maintenance, routing maintenance, maintenance schedules, maintenance personnel log, and service level agreements (SLA), if applicable.* | * System-specific system maintenance procedures addressing all maintenance requirements * SLAs or maintenance contracts, if applicable |  |
| MA-3 | * What types of records are maintained? | *Maintenance records should be maintained. Maintenance logs should be protected from unauthorized modification and deletion.* | * Maintenance log * Audit records showing maintenance activities associated with the User ID of individual performing maintenance * SLAs or maintenance contracts, if applicable |  |
| MA-2 MA-3 | * What agreements or arrangements regarding diagnostic equipment and software that vendors may bring onsite exist? * How is it monitored? * Are you aware of how access to tools is restricted to MA personnel? | *System-specific MA procedures should clearly define how third-party maintenance will be performed and what appropriate controls are in place to ensure that only authorized personnel perform authorized (and approved) maintenance activities. The AC policy should include specific access restrictions when external services and equipment are allowed within the system.* | * Maintenance logs * Maintenance SLAs or maintenance contracts, if applicable * Access control demonstrating authorized activities of external maintenance contractors are monitored |  |
| MA-4 | * What ability do vendors have to perform remote diagnostics and maintenance? * How is remote diagnostics and maintenance authorized, monitored, and controlled? * Are records for remote maintenance maintained? * Can you provide a few maintenance records? | *System-specific procedures documenting security controls in place for implementing and monitoring remote maintenance.* | * Formal approval authorizing remote maintenance * System generated audit records for remote maintenance |  |
| MA-5 | * What type of tracking is done for personnel authorized to perform MA on the information systems? * Is there a list of authorized personnel? Who has access to the list? * How are MA personnel verified? * Request to see the list. | *List of authorized MA personnel should be kept current.* | * List of MA personnel |  |
| MA-6 | * Describe SLAs with MA vendors (turn-around time). * Are there any spare parts stored onsite? * Where onsite are spare parts stored? * Is there a documented MA schedule? | *Third-party SLAs, if applicable, should be maintained and reviewed periodically.* | * SLAs |  |

# Contingency Planning

Contingency Planning prepares for, responds to, and recovers from disruptions to ensure mission or business continuity.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 the component recovery prioritization? | *Detailed recovery process for system components should be documented and the administrator should be trained in fulfilling CIO’s CP role.* | * CP document and description of SysAdmins’ roles and responsibilities in related areas |  |
| CP-3 | * What are your CP roles and responsibilities? * Have you received training? * How often is training performed? | *Detailed recovery process for system components should be documented and the administrator should be trained in fulfilling CIO’s CP role. Administrators supporting various system components should be training at least once every 365 days or when necessary.* | * Training records of SysAdmins (for all system components) |  |
| CP-4 | * What involvement have you had in any CP tests or exercises? * Describe how these CP tests or exercises were conducted and the scenarios encompassed. | *CP testing should be conducted at least once every year or when contingency criteria changes due to changes within business (or system) circumstances. At the minimum, tabletop exercises must be performed to identify any deficiencies in the recovery priorities and to ensure that the plan will work as intended.* | * Examine current tabletop test results showing that the administrator’s role DR/CP testing has been executed successfully (tabletop sign-offs, etc.) |  |
| CP-6 | * Where is your system’s backup information stored? Is it offsite? * What information is stored at the offsite? * How are databases kept in sync between the primary and backup data center? * How is the code base synchronized (e.g., is a production change deployed in primary, as well as backup, or is primary periodically cloned? | *Data should be backed up at the alternate storage site to facilitate system recovery point objective (ROP).* | * Examine the log showing date and time when the backup tapes are transferred to an alternate storage site |  |
| 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 the alternate storage site? * Are the tapes encrypted? * What is backup tape rotation frequency? * How are backups protected during transit and at offsite storage? * Are backups periodically tested and if so, 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 tapes; and criteria for alternate storage. The backup of system configurations and data should be performed to support the system RPO.* | * Formally documented system-specific backup procedure and records |  |
| CP-10 | * Where are the recovery procedures documented? * Describe the recovery process for the equipment/systems you are responsible for (i.e., reload operating system, apply patches, apply baseline configurations, etc.). * What types of assumptions do your procedures assume (backup media will be available, like equipment, etc.)? * Where are your recovery procedures, and are they accessible during an emergency? | *System-specific recovery and reconstitution steps and priorities should be clearly documented in the CP.* | * System-specific configuration baseline document describing system components (i.e. hardware and software), system parameter settings, and patch requirements |  |

# Media Protection

Media Protection protects physical and digital media containing sensitive data from unauthorized access or disclosure.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control(s) | Question(s) | Guidance | Evidence Examples | Response |
| MP-1 | * Describe your knowledge of the organization’s:   + Formal, documented MP policy that addresses purpose, scope, roles, responsibilities, and compliance   + Formal, documented procedures to facilitate the implementation of the MP policy and associated MP controls, including both electronic (backup media, thumb drives, etc.) and paper output | *The organization’s MP policy should be followed.* | * System-specific procedures to restrict access to digital and non-digital media |  |
| MP-3 | * Observe and Interview to determine whether external labels are affixed to removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings of the information. * If no external labels are affixed, was a risk analysis performed, or other process followed to arrive at the decision? | *System-specific formally documented MP procedures should be in place addressing media marking requirements.* | * Examine appropriate markings on digital and non-digital media |  |
| MP-4 | * How is sensitive (PII or PHI) contained in electronic media (backup, thumb drive) controlled/accessed? * Is the information system media protected by cryptography (NIST SP 800-66 has guidance)? * Was a risk analysis performed, or other process followed to arrive at the decision? | *Digital/electronic media should be encrypted and/or locked appropriately. Non-digital media should be handled as per the organization’s security policy.* | * Review media storage and media encryption procedures |  |
| MP-6 | * How is information system media, both digital and non-digital, sanitized prior to disposal or release for reuse? * Is electronic media sanitized in accordance with best practices (NSA Guidance and NIST SP 800-88)? * Is sanitization tracked and documented? * Are media sanitization mechanisms and strength of the tools used appropriate to the classification and sensitivity of the information residing on the media? | *MP procedures should be documented describing the types of media sanitization techniques used and person authorized to sanitize the media prior to disposal or reuse.* | * System-specific MP procedures describing tools and techniques |  |

# System and Communications Protection

System and Communications Protection protects the integrity, confidentiality, and availability of transmitted and stored information.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control(s) | Question(s) | Guidance | Evidence Examples | Response |
| 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? | *Cryptographic requirements supporting system communications and key management procedures should be documented in the SSP. The system may be dependent on the GSS for these services, but this should be clearly stated in the SSP.* | * Key management procedures |  |