

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>)

Application Developer  
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. Security Policy and Procedures 1](#_Toc199483138)

[2. Access Control and Identification and Authentication 2](#_Toc199483139)

[3. Audit and Accountability 5](#_Toc199483140)

[4. System and Information Integrity 9](#_Toc199483141)

[5. Incident Response 10](#_Toc199483142)

[6. Awareness and Training 11](#_Toc199483143)

[7. Configuration Management 12](#_Toc199483144)

[8. System and Services Acquisition 13](#_Toc199483145)

[9. Contingency Planning 15](#_Toc199483146)

[10. Media Protection 16](#_Toc199483147)

[11. System and Communications Protection 17](#_Toc199483148)

# 

# Security Policy and Procedures

Provide an overview of your roles and responsibilities related to the application or system, as well as the controls in place to secure it. Include all application or system components for which you have a specific responsibility to ensure security.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control(s) | Question(s) | Guidance | Evidence Examples | Response |
| All “-1” Controls | * How are the policies and procedures disseminated to staff? * How often do you receive information on updates? * If you have a question on how the control should be implemented, what sources would you use to clarify the organization’s implementation? | *All staff should be familiar with the organization’s policies and capable of referencing the location of the policy and associated procedures. This question should be asked of all interviewees.* | * N/A |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Access Control and Identification and Authentication

Ensure that there are no unapproved users/IDs, unauthorized access to, exposure of, or modification to data and systems in the controlled environment.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control(s) | Question(s) | Guidance | Evidence Examples | Response |
| AC-1 | * Describe the access control policies and procedures and their implementation in relation to the application/ system. | *System specific account access controls should be documented, and the developer should understand how it works to limit access to the application.* | * Formally documented description of the access control in place for the application that was considered in the development of the application |  |
| AC-3 | * Describe any access control that is controlled by the application. * How is access control implemented and maintained for the application? * Who is in charge of granting access to the application and updating application specific security if it does exist? | *the application may be totally dependent on the infrastructure for access control or there may be additional access control mechanisms built within the application. If supported within the application the developer should know what role(s) has this capability.* | * Documentation on the application access control mechanisms |  |
| AC-5 | * Describe your access to any application source, data or configuration files in the production environment * How does the application enforce separation of duties? * To what groups/roles are users assigned? * What privileges are granted to developers? * How does the application 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 | * How do application developers use remote access to support and maintain the application? * What is the process to obtain authorization for remote 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) |  |
| IA-2 | * How are users uniquely identified and authenticated? * How was the application e-authentication level determined? * How is the multi-factor authentication requirement implemented for this information system for both privileged and non-privileged accounts? * What are the two factors of authentication that are used to access the system? * What certificates are used? * Does the application allow the use of group accounts? * 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 |  |

# Audit and Accountability

Ensure that information is retained to support after-the-fact investigations of security incidents and to provide accountability for actions in relation to system events

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control(s) | Question(s) | Guidance | Evidence Examples | Response |
| AU-1 | * Explain all auditing performed by the application, 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 do 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 application specific audit or transaction records used to investigate security incidents? * 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 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 or transaction records/reports produced from Production application to see what events are being logged and how many details are logged for each event * Request records or report that reflect the activity performed by the Application Evaluator from the test environment |  |
| AU-4 AU-5 AU-11 | * How were you involved in determining the storage requirements for the application 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 application stopped capturing audit records or transaction history? * What type of notification (an alert/notification) would you receive 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 application audit or transaction history information. * Is automation used? * Is a weekly, daily, and/or monthly reports generated? * Are any aggregation and correlation of events performed? * 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—confirm 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 day * Evidence that demonstrates each event was responded to within the established timeframes and closed (*i.e.* Email, wet signature) * 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 with internal information systems performed? | *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 or transaction history information (i.e., online logs and archived) and audit tools? | *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

The objective is to ensure that systems are designed using secure software engineering principals and remain secure by addressing critical security flaws.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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? | *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? * What is the process (start to finish) from flaw remediation notification to installation in the Production Environment? * How are software fixes distributed across systems? | *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 |  |

# 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. * Are they documented? * 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 IR policy. Incident Response capability planning activities should be coordinated between System Owner, ISSO, BO, and other relevant individuals supporting the system.* | * Incident response policy and guidance * System-specific IR procedures, if applicable |  |
| IR-5 IR-7 | * To whom does staff report incidents to? * How are incidents information collected/documented (i.e., automated system/database for future correlation)? * Is there a help desk support function that users can report suspected incidents? | *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 |  |

# 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 application * Are there areas that the documented policy does not address, such as testing the modified application updating the Version description document? | *The organization’s CM policy should be followed.* | * System-specific formally documented CM procedures |  |
| CM-3 | * Describe 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 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 |  |

# System and Services Acquisition

System and Services Acquisition integrates security into the acquisition and development lifecycle of systems and services.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control(s) | Question(s) | Guidance | Evidence Examples | Response |
| SA-8 | * What familiarity do you have with the security engineering principles detailed in NIST SP 800-27 Revision A, Engineering Principles for IT Security (A Baseline for Achieving Security)? * What security principles were used in the development of this application? | *The developer should have knowledge of security engineering principles and be able to discuss how they were used in the development of the application.* | * Coding or application development standards which incorporate security engineering principles |  |
| SA-10 | * Describe the developers’ configuration management plan that controls changes during development, tracks security flaws, requires authorization of changes, and provides the documentation of the plan and its implementation. * How is CM handled during the development process to ensure proper testing of controls? * What type of data is used for testing? Is PII used to test the system in the development region? * How do you ensure that security as designed is implemented in the system? * Do you have a Security Test and Evaluation Plan or test scripts which focus on testing the security controls implemented and how are the results of the tests? | *To ensure that security controls incorporated into an application which could include the separation of functions based on role, the developers should control code changes so that testing can be done during development. Request a copy of the test plan which must highlight testing of security controls both within the application and associated within the operating environment that are inherited by the application.* | * Developer configuration management process * Developer procedures |  |

# 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 CP tests or exercises have you participated? * Describe how these CP tests or exercises were conducted and the scenarios they 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.) |  |

# 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-3 | * Observe and Interview to determine whether external labels are affixed 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 |  |

# 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 |  |