

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>)

Database Administrator  
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](#_Toc199483370)

[2. Audit and Accountability 6](#_Toc199483371)

[3. System and Information Integrity 10](#_Toc199483372)

[4. Incident Response 12](#_Toc199483373)

[5. Awareness and Training 13](#_Toc199483374)

[6. Configuration Management 14](#_Toc199483375)

[7. Maintenance 16](#_Toc199483376)

[8. Contingency Planning 17](#_Toc199483377)

# 

# 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 database access? * What is the process for establishing and activating accounts? * What is the process for modifying access to the database, (e.g., What is the process for someone with read-only access that now has a need for update access?)? * What is the process for disabling and removing accounts with access to the database both administrators and users (e.g., if an employee quits, how is the account removed from the application/system?)? * What is the process followed for emergency terminations, in particular for database administrators? * Are accounts actually deleted or is there a need to retain accounts for historical purposes? | *Formally documented system-specific database 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 database access, the database’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 database 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 database 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 the database * List of active users and system-generated record of userIDs 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 database administrator? * What are the escalation procedures should there be an issue? * When are inactive accounts disabled; what is the period of inactivity? * 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 | * How are temporary and/or default system (or service) accounts handled after the database is installed or software is updated? | *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? * What groups/roles are assigned to support separation of duties? * What privileges are granted to database administrators? | *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 the database is permitted? * What is the process to obtain authorization for remote access? * How is multifactor authentication used for remote access? * Who is authorized to remotely access the database? * How is access monitored? * Is there an automated audit capability to log the activities associated with remote access? | *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 organization’s 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-19 | * What authorized users’ personal computers/devices to access the database is allowed? | *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 |  |
| IA-2 | * How are database administrators and users uniquely identified and authenticated? 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 |  |

# 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 database, 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 database 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 database audit records used to investigate possible security incidents? * What database events are tracked and how were the events determined? * What information is captured (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 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 database 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 database 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. * What is the process, who performs the review, and how often is the review performed? * 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? * How are access controls (i.e., accounts, access to directories/files) reviewed to ensure they are working/set as intended? * How often are database administrator level groups and level accounts reviewed? * 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? * What is the frequency of report generation (i.e. weekly, daily, and/or monthly)? * What patterns are looked for in the data when the review is performed? * How are the events shared with the organization’s business owner (BO) and Chief Information Security Officer (CISO)? | *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 day * 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-9 | * Who has access to database audit information (i.e., online logs and archived) and audit tools? * How is database 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 database audit information retained? * Where is the database 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 in the database? | *The information should be included in the design documentation or SSP* | * Rules for the tools or mechanisms in place |  |
| SI-2 | * How do you become aware of patches, hot fixes, and service packs to remediate database 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-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 |  |

# 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. * Describe any procedures associated with 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-2 | * Describe any IR training you receive. * 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-5  IR-7 | * To whom does staff report incidents to? | *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 role-based, 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 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 database baseline configurations developed and documented? * How often is the baseline updated? * 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 database? * 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 |  |

# 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-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 |  |

# 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 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.) |  |
| 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 (RPO).* | * Examine the log showing date and time when the backup tapes are transferred to an alternate storage site |  |
| CP-9 | * What types of database backups are done? * 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 database 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 * System-specific MP procedures describing tools and techniques |  |