

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>)

Security Assessment Plan (SAP)

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. |

**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.

Table of Contents

[1. Introduction 1](#_Toc198586421)

[2. System Information 1](#_Toc198586422)

[2.1 Brief Description of System 1](#_Toc198586423)

[2.2 System Identification and Security Level 1](#_Toc198586424)

[2.3 Responsible Organizations 1](#_Toc198586425)

[2.4 System Type Designation and Categorization/Classification 2](#_Toc198586426)

[2.5 System Operational Status 3](#_Toc198586427)

[3. Security Assessment Scope 3](#_Toc198586428)

[3.1 Boundary Descriptions 3](#_Toc198586429)

[3.1.1 Authorization Boundary Description 3](#_Toc198586430)

[3.1.2 Assessment Boundary Description 6](#_Toc198586431)

[3.1.3 Prioritized Assessment 12](#_Toc198586432)

[3.1.4 Core Controls 12](#_Toc198586433)

[3.2 Application Testing Requirements 13](#_Toc198586434)

[3.2.1 Access Mechanisms/Locations 14](#_Toc198586435)

[3.3 Assumptions/Limitations 14](#_Toc198586436)

[3.4 Points of Contact & Assessment Roles 15](#_Toc198586437)

[4. Requirements and Schedule 17](#_Toc198586438)

[4.1 Physical Access and Work Area Requirements 17](#_Toc198586439)

[4.2 Artifact Requirements 17](#_Toc198586440)

[4.2.1 Tier 1 Artifacts – Minimum Security Artifacts 18](#_Toc198586441)

[4.2.2 Tier 2 Artifacts – Supporting Artifacts 18](#_Toc198586442)

[4.3 Technical Output Artifacts 22](#_Toc198586443)

[4.4 Security Assessment Schedule 23](#_Toc198586444)

[4.5 Security Assessment Estimated Timeline 24](#_Toc198586445)

[5. ACT Security Assessment Process and Methodology 24](#_Toc198586446)

[5.1 Assessment Phases 25](#_Toc198586447)

[5.1.1 Phase 1: Planning 25](#_Toc198586448)

[5.1.2 Phase 2: Assessment 25](#_Toc198586449)

[5.1.3 Phase 3: Reporting 26](#_Toc198586450)

[5.2 Roles and Responsibilities 26](#_Toc198586451)

[5.2.1 Application Developer/Maintainer 26](#_Toc198586452)

[5.2.2 Security Assessment Lead 26](#_Toc198586453)

[5.2.3 Business Owner 27](#_Toc198586454)

[5.2.4 Configuration Manager 27](#_Toc198586455)

[5.2.5 Contingency Planning Manager 27](#_Toc198586456)

[5.2.6 Database Administrator 27](#_Toc198586457)

[5.2.7 Datacenter / Facilities Manager 28](#_Toc198586458)

[5.2.8 Development Lead 28](#_Toc198586459)

[5.2.9 Firewall Administrator 28](#_Toc198586460)

[5.2.10 Human Resources Manager 28](#_Toc198586461)

[5.2.11 Incident Handling Manager 28](#_Toc198586462)

[5.2.12 Information System Security Manager 29](#_Toc198586463)

[5.2.13 Information System Security Officer or Information System Security Manager 29](#_Toc198586464)

[5.2.14 Mainframe Administrator 29](#_Toc198586465)

[5.2.15 Media Custodian 29](#_Toc198586466)

[5.2.16 Middleware Utilities Administrator 30](#_Toc198586467)

[5.2.17 Network Administrator 30](#_Toc198586468)

[5.2.18 Privacy Subject Matter Expert 30](#_Toc198586469)

[5.2.19 Program Manager 30](#_Toc198586470)

[5.2.20 Security Utilities Administrator 31](#_Toc198586471)

[5.2.21 System Administrator 31](#_Toc198586472)

[5.2.22 System Owner 31](#_Toc198586473)

[5.2.23 Training Manager 31](#_Toc198586474)

[5.3 Security Assessment Activities 31](#_Toc198586475)

[5.3.1 Level of Testing Rigor 32](#_Toc198586476)

[5.3.2 Documentation Review 33](#_Toc198586477)

[5.3.3 Application Testing 33](#_Toc198586478)

[5.3.4 Database Server/Instance Testing 35](#_Toc198586479)

[5.3.5 Interviews 36](#_Toc198586480)

[5.3.6 Network Scans 36](#_Toc198586481)

[5.3.7 Penetration Testing 37](#_Toc198586482)

[5.3.8 Wireless Assessment 37](#_Toc198586483)

[5.3.9 Configuration Review 37](#_Toc198586484)

[5.3.10 Observances 37](#_Toc198586485)

[5.3.11 Mainframe Batch Process Testing 38](#_Toc198586486)

[5.3.12 Mainframe System Testing 38](#_Toc198586487)

[5.4 Reporting 39](#_Toc198586488)

[5.4.1 Findings Worksheet 39](#_Toc198586489)

[5.4.2 Reassignment of Findings 39](#_Toc198586490)

[5.4.3 Rating of SQL Injection and XSS Vulnerabilities 39](#_Toc198586491)

[5.4.4 Test Reporting 39](#_Toc198586492)

[5.4.5 Remediation Period 40](#_Toc198586493)

# 

# Introduction

This document describes the Adaptive Capabilities Testing (ACT) Security Assessment methodology, schedule, and requirements that <Name of ACT Contractor> (“the Assessment Team”) will use to evaluate the <System Name> (<System Acronym>) General Support System (GSS) and/or Major Application (MA)>. <System Acronym> is owned by <division / group within sponsor organization> and <operated/developed/maintained/etc.> by <Contractor>.

The purpose of this ACT Security Assessment Plan is to clearly explain the information the Assessment Team needs to obtain prior to the assessment, the areas that will be examined during the assessment, and the proposed schedule of activities the Assessment Team expects to perform during the assessment. This document is meant to be used by the <Organization> and contractor personnel responsible for the security of the system (the “System Team”).

# System Information

## Brief Description of System

<Brief description of the system.>

## System Identification and Security Level

Table 1. System Identification

|  |  |
| --- | --- |
| Official System Name | * Official System Name |
| System Acronym | * ABCD |
| System Purpose | * <Brief summary of the system’s purpose of the system – 1 to 2 sentences.> |
| System of Records (SOR) ID | * 12345 |
| Financial Management Investment Board (FMIB) Number | * 67890 |

## Responsible Organizations

Table 2. Responsible Organizations

|  |  |
| --- | --- |
| Authorizing Official | * <Organization> Chief Information Security Officer (CISO) |
| System Owner / Responsible Organization | * <Organization> / RX93 – Enterprise Information Technology Division Office |
| System Contractors & Roles | * ABC Contractor: Development * DEF Contractor: Maintenance * GHI Contractor: Hosting |

## System Type Designation and Categorization/Classification

Table 3. System Type Designation and Categorization/Classification

|  |  |
| --- | --- |
| System Type | * Major Application (MA) * General Support System (GSS) * Cloud Service Provider (CSP) * Standalone (SUSA) * Multi-User Standalone (MUSA) * Closed Restricted Network (Local Area Network (LAN)) * Wide Area Network (WAN) * Interconnected System – Contractor-to-Contractor (C2C) * Interconnected System – Contractor-to-Government (C2G) * <Other System Type> |
| High Value Asset (HVA) | * Yes/No |
| FIPS 199 Security Category | * Overall: Low / Moderate / High * Confidentiality: Low / Moderate / High / Not Applicable * Integrity: Low / Moderate / High / Not Applicable * Availability: Low / Moderate / High / Not Applicable |
| FIPS 199 Security Category Rationale | * <Rationale – explain how the ratings for the Security Objectives and overall Security Category were determined> |
| Sensitivity Level (of System and/or Hosted Data) | * Public Trust (PT) * Confidential * Personally Identifiable Information (PII) * Protected Health Information (PHI) * Financial Data |
| Classification Level (of System and/or Hosted Data) | * Unclassified * Controlled Unclassified Information (CUI) * Secret * Top Secret * <Other Classification Level> |
| Classification Caveats | * None * FRD * RD * FGI * <Other> |
| Classification Formal Access Approvals | * None * NATO * COMSEC * CNWDI * <Other> |
| System User / Development Personnel Minimum Clearance | * Confidential * Secret * Top Secret |
| System User / Development Personnel Minimum Access | * Interim * Final |
| System User / Development Personnel Citizenship | * US-only * Foreign Nationals: <Specify Nationalities> |

## System Operational Status

Table 4. System Operational Status

|  |  |
| --- | --- |
| Operational Status | * Under Development * New * Operational * Undergoing a Major Modification * <Other> |

# Security Assessment Scope

## Boundary Descriptions

“What will and won’t be assessed?”

The reader should be able to clearly understand what is in scope for the assessment and the details provided throughout the document must remain consistent with that defined scope. Using plain language, define and/or depict any deviations from the System Security Plan’s authorization boundary and the assessment’s intended scope.

### Authorization Boundary Description

The system’s official authorization boundary diagram from the System Security Plan (SSP) is shown in Figure 1.

Copy/paste the system’s official accreditation boundary diagram from the SSP (or other official source). Ensure that the pasted diagram is of sufficient resolution and quality to be legible and useful to the reader. If it cannot be made legible and useful, add a note explaining why.

Make no edits to the official diagram here – if edits are needed, document them in updated versions of the diagram later in this section (see template language). The official authorization boundary diagram should:

1. Provide a last-updated date and legend
2. Clearly define its own authorization boundary
3. Identify equipment/component inventory consistent with documented hardware and software inventories (to include the most recent configuration of firewalls, Intrusion Detection or Prevention Systems (IDS/IPS), routers, switches, Internet Protocol (IP) addresses, encryption devices, etc.
4. Identify any other cybersecurity or cybersecurity-enabled products deployed in the boundary/enclave
5. Identify any connections to other systems/networks/enclaves, including:

* The name of the organization that owns the system/network/enclave
* The connection type (e.g., wireless, dedicated point-to-point, etc.)
* The organization type (e.g., MITRE, federal agency, contractor, etc.)

1. Include the model numbers and IP addresses of the devices on the diagram; diagram must show actual and planned interfaces to internal and external LANs or WANs

* Data flows should be clearly indicated
* Protocols utilized by IP connections should be defined

A screenshot of a cell phone

Description automatically generated

Figure . <System Acronym> Official Authorization Boundary Diagram

If the official diagram, when pasted into this template, does not clearly and unambiguously identify the accreditation boundary as described in the guidance above, then mark up the diagram and/or add verbiage to clarify the accreditation boundary. This will then be followed by the Scope table which defines what was and wasn’t in-scope for this particular assessment of that (potentially larger) accreditation boundary.

Because the official authorization boundary diagram from the SSP is difficult to read and does not clearly identify the authorization boundary, the Assessment Team worked with <System Acronym> personnel to clarify the authorization boundary, resulting in the following updated authorization boundary diagram that was created by the Assessment Team and confirmed and approved by the <System Acronym> team prior to the start of the assessment phase. The clarified authorization boundary is shown inside the green dashed boxes in Figure 2:

A screenshot of a cell phone

Description automatically generated

Figure . <System Acronym> Updated Authorization Boundary Diagram

### Assessment Boundary Description

Based on the above definition of the authorization boundary, the <System Acronym> team directed the Assessment Team to assess [the entire system / certain portions of the system], as shown by the red dashed boxes in Figure 3:

A screenshot of a map

Description automatically generated

Figure . <System Acronym> Assessment Boundary Diagram

If applicable, the following should clearly notate any deviations between the authorization boundary as defined by the SSP, the clarified/updated authorization boundary (if applicable), and the assessment’s intended scope. List components as identified in the authorization boundary diagram.

The following objects/components that fall within the system’s [official / updated] authorization boundary are excluded from assessment during this [comprehensive-scope / tailored-scope] ACT Security Assessment:

* Component 1
* Component 2
* Application 1
* Application 2

The following tables detail System Information and the Assessment Boundary of this ACT Security Assessment:

The author must ensure consistency across all sections of this document. If a row’s requested information is out of scope for this assessment, clearly mark that section as “**Not in scope**”.

Table . In-Scope Portions of Authorization Boundary

|  |  |
| --- | --- |
| Applications | * ABCD Main Application: Web Server 1, Web Server 2 * EFGH Supporting Application: Web Server 2 |
| Database Servers & Instances | * PRODDB01: Oracle 11i. * ABCD accounts payable database: Oracle 11i. * EFGH database: SQL Server 2013. * PRODDB04: SQL Server 2013 * ABCD accounts receivable database: Oracle 11i |
| Servers / Workstations & Operating Systems | * PRODDB01: Solaris 11.2 * PRODDB04: Windows Server 2013 R2 * PRODAPP01: Red Hat Enterprise Linux 6.6 |
| Any Mainframe-based Components Being Assessed? | * Yes / No |
| Network Devices / Infrastructure | * 192.168.1.25 (“Load Balancer”): SuperMax HyperBalance LB * 192.168.5.30 (“Switch”): Cisco 5620 Switch * 192.168.1.1 (“Firewall” at Internet/DMZ border): WatchGuard X45 * 192.168.5.1 (“Firewall at DMZ/Data Zone border): Sophos AV-FW Xtreme |
| Cloud Technologies | * Amazon Data Lake: Amazon S3 * Amazon Data Lake: AWS Lake Formation * Amazon Data Lake: Amazon Athena * Azure DevOps: Azure Pipelines * Azure DevOps: Azure Boards * [Other] |
| Cloud Services | * Amazon Data Lake * Amazon Virtual Private Cloud * Azure DevOps * Azure Data Factory * [Other] |
| Virtualization/Hypervisor Technologies | * Hyper-V Server 2019 * Red Hat Virtualization Hypervisor v4.4 * VirtualBox 7.0.10 * VMware ESX * [Other] |
| Other Technologies | * XYZ Tech |
| Interconnections | * System Name – System Owner |
| Required Authentication Methods | * LDAP * RADIUS * TACACS / TACACS+ * Active Directory (AD) * Local Authentication * Resource Access Control Facility (RACF) |

Table . ACT Security Assessment Scope Specification

|  |  |
| --- | --- |
| Assessment Type | * Comprehensive ACT (Application + Infrastructure) * Comprehensive ACT (Application-Only) * Comprehensive ACT (Infrastructure-Only) * Tailored Scope ACT (Application + Infrastructure) * Tailored Scope ACT (Application-Only) * Tailored Scope ACT (Infrastructure-Only) * Tailored Scope (FISMA 1/3) ACT (Application + Infrastructure) * Tailored Scope (FISMA 1/3) ACT (Application-Only) * Tailored Scope (FISMA 1/3) ACT (Infrastructure-Only) |
| Core Controls / Capabilities Included? (If not, explain why not) | * Yes / No |
| Testing Rigor | * Level 1: Assertion Appropriateness * Level 2: Passive Compliance Verification * Level 3: Basic Compliance Verification * Level 4: Advanced Compliance Verification |
| Security Capabilities / Sub-Capabilities  If no Sub-Capabilities are listed, then all Sub-Capabilities for that Capability are included. | * BEHAVE: Manage Behavioral Expectations   + BEHAVE-01, BEHAVE-05 * BOUNDE: Manage Cryptographic Mechanisms Controls * BOUNDF: Manage Network Filters and Boundary Controls * BOUNDP: Manage Physical Access Controls * CRED: Manage Credentials and Authentication * CSM: Configuration Settings Management * DBS: Design and Build-in Security * HWAM: Hardware Asset Management * MNGEVTAU: Manage Events for Audit and Accountability * MNGEVTCP: Manage Events for Contingency Planning * MNGEVTIR: Manage Events for Incident Response * MNGEVTOA: Manage Events for Ongoing Assessment * MNGEVTP: Manage Events for Privacy * PRIV: Manage Privileges and Accounts * RISK/OMI: Manage and Assess Risk / Operate, Monitor, Assess (OMI) * SWAM: Software Asset Management * TRUST: Manage Trust for Persons Granted Access * VULN: Vulnerability (Patch) Management   **Sub-Capabilities List Compatible with recommended “FISMA 1/3” Schedule:**  **Year 1**   * BEHAVE: Manage Behavioral Expectations * BOUNDE: Manage Cryptographic Mechanisms Controls * BOUNDP: Manage Physical Access Controls   + BOUNDP-01 * CRED: Manage Credentials and Authentication * CSM: Configuration Settings Management   + CSM-01, CSM-02, CSM-03, CSM-04, CSM-05, CSM-06, CSM-07, CSM-08, CSM-09, CSM-10, CSM-12, CSM-13 * DBS: Design and Build-in Security * HWAM: Hardware Asset Management * MNGEVTAU: Manage Events for Audit and Accountability * MNGEVTCP: Manage Events for Contingency Planning   + MNGEVTCP-01, MNGEVTCP-02, MNGEVTCP-06, MNGEVTCP-07 * MNGEVTIR: Manage Events for Incident Response * MNGEVTOA: Manage Events for Ongoing Assessment * MNGEVTP: Manage Events for Privacy * PRIV: Manage Privileges and Accounts * RISK/OMI: Manage and Assess Risk / Operate, Monitor, Assess (OMI)   + RISKOMI-05, RISKOMI-07 * SWAM: Software Asset Management * TRUST: Manage Trust for Persons Granted Access   + TRUST-01, TRUST-02, TRUST-03, TRUST-04, TRUST-06, TRUST-09, TRUST-10   **Year 2**   * BEHAVE: Manage Behavioral Expectations * BOUNDE: Manage Cryptographic Mechanisms Controls   + BOUNDE-01, BOUNDE-03, BOUNDE-04 * BOUNDF: Manage Network Filters and Boundary Controls   + BOUNDF-01, BOUNDF-02, BOUNDF-03, BOUNDF-04, BOUNDF-05, BOUNDF-06, BOUNDF-07, BOUNDF-08 * BOUNDP: Manage Physical Access Controls * CRED: Manage Credentials and Authentication * CSM: Configuration Settings Management   + CSM-01, CSM-03, CSM-04, CSM-05, CSM-06, CSM-07, CSM-08, CSM-09, CSM-10, CSM-11, CSM-12, CSM-13 * DBS: Design and Build-in Security * HWAM: Hardware Asset Management * PRIV: Manage Privileges and Accounts * RISK/OMI: Manage and Assess Risk / Operate, Monitor, Assess (OMI)   + RISKIOMI-05, RISKOMI-06 * SWAM: Software Asset Management * TRUST: Manage Trust for Persons Granted Access   **Year 3**   * BEHAVE: Manage Behavioral Expectations * BOUNDE: Manage Cryptographic Mechanisms Controls   + BOUNDE-01, BOUNDE-03, BOUNDE-04 * BOUNDF: Manage Network Filters and Boundary Controls * CRED: Manage Credentials and Authentication * CSM: Configuration Settings Management   + CSM-01, CSM-03, CSM-04, CSM-05, CSM-06, CSM-07, CSM-08, CSM-09, CSM-10, CSM-12, CSM-13 * DBS: Design and Build-in Security * HWAM: Hardware Asset Management * PRIV: Manage Privileges and Accounts * RISK/OMI: Manage and Assess Risk / Operate, Monitor, Assess (OMI) * SWAM: Software Asset Management * TRUST: Manage Trust for Persons Granted Access   + TRUST-01, TRUST-03, TRUST-04, TRUST-06, TRUST-07, TRUST-08 * VULN: Vulnerability (Patch) Management |
| Security Control Families / Controls  If no Controls are listed, then all Controls for that Control Family are included. | * AC: Access Control   + AC-01, AC-05, AC-11 * AP: Authority and Purpose * AR: Accountability, Audit, and Risk Management * AT: Awareness and Training * AU: Audit and Accountability * CA: Security Assessment and Authorization * CM: Configuration Management * CP: Contingency Planning * DI: Data Quality and Integrity * DM: Data Minimization and Retention * IA: Identification and Authentication * IP: Individual Participation and Redress * IR: Incident Response * MA: Maintenance * MP: Media Protection * PE: Physical and Environmental * PL: Planning * PM: Program Management * PS: Personnel Security * RA: Risk Assessment * SA: System and Services Acquisition * SC: System Communications * SE: Security * SI: System and Information Integrity * TR: Transparency * UL: Use Limitation   **Controls List Compatible with recommended “FISMA 1/3” Schedule:**  **Year 1**   * AC: Access Control * AP: Authority and Purpose * AR: Accountability, Audit, and Risk Management * AT: Awareness and Training * AU: Audit and Accountability * CM: Configuration Management * CP: Contingency Planning * DI: Data Quality and Integrity * DM: Data Minimization and Retention * IA: Identification and Authentication * IP: Individual Participation and Redress * SC: System Communications * SE: Security * TR: Transparency * UL: Use Limitation   **Year 2**   * AC: Access Control * AT: Awareness and Training * AU: Audit and Accountability * CM: Configuration Management * IA: Identification and Authentication * MA: Maintenance * MP: Media Protection * PE: Physical and Environmental * PM: Program Management * PS: Personnel Security   **Year 3**   * AC: Access Control * AP: Authority and Purpose * AR: Accountability, Audit, and Risk Management * CA: Security Assessment and Authorization * CM: Configuration Management * DI: Data Quality and Integrity * DM: Data Minimization and Retention * IA: Identification and Authentication * IP: Individual Participation and Redress * IR: Incident Response * PL: Planning * RA: Risk Assessment * SA: System and Services Acquisition * SE: Security * SI: System and Information Integrity * TR: Transparency * UL: Use Limitation |
| Assessment Environments | * Production: databases, operating systems, network infrastructure, security infrastructure * Testing: application |
| Environment Hosting Locations | * Production: Amazon Web Services (AWS) us-east-1 * Testing: Primary Data Center (PDC) * [Other] |
| Existing Open POA&Ms to be Reassessed | * Open-POA&M-Tracking-IDs |
| Assessment Dates | * May 5 – 9, 2025 |
| Assessment Location(s) | * Interviews: Remote via [mechanism] * Testing: <Organization> Primary Data Center (PDC) * <Address> * [Other] |
| Assessment Standards / Checks | * <Sponsor-specified Security Controls Catalog> * FedRAMP High / Moderate / Low * Industry Best Practices * [Others…] |

### Prioritized Assessment

**“What is <Organization> concerned with going into the ACT?”**

If <Organization> requested that any components, features, functions, etc. of the system be focused on or otherwise prioritized as part of the assessment, list them here. This will help to explain why some parts get more attention than others.

<Organization> directed the Assessment Team to prioritize assessment of the following components/features/functions/etc. because:

* <System Component/Feature/Function>: <Reason for prioritization>
* <System Component/Feature/Function>: <Reason for prioritization>
* <System Component/Feature/Function>: <Reason for prioritization>

### Core Controls

The <System Acronym> team also prioritized assessment of the <Organization> Core Controls, a periodically updated list of the controls that pose the highest risk to <Organization> as a whole. At the time of this ACT Security Assessment, the <Organization> Core Controls are:

Table . <Organization> Core Controls at Time of Assessment

| **Control ID** | **Control Name** |
| --- | --- |
| AC-01 | Access Control Policy and Procedures |
| AC-02 | Account Management |
| AC-03 | Access Enforcement |
| AC-05 | Separation of Duties |
| AC-06 | Least Privilege |
| AC-17 | Remote Access |
| CA-03 | System Interconnections |
| CM-02 | Baseline Configuration |
| CM-03 | Configuration Change Control |
| CM-06 | Configuration Settings |
| CM-07 | Least Functionality |
| CP-02 | Contingency Plan |
| CP-03 | Contingency Training |
| CP-04 | Contingency Plan Testing |
| CP-04(01) | Coordinate with Related Plans |
| IA-02 | Identification and Authentication |
| IA-05 | Authenticator Management |
| IR-05 | Incident Monitoring |
| IR-06 | Incident Reporting |
| IR-06(01) | Automated Reporting |
| PL-02 | System Security Plan |
| SC-07 | Boundary Protection |
| SC-08 | Transmission Confidentiality and Integrity |
| SC-13 | Cryptographic Protection |
| SC-28 | Protection of Information at Rest |
| SI-02 | Flaw Remediation |

## Application Testing Requirements

Customize this section based on the assessment’s scope.

Test accounts that reflect the different user types and roles must be created and verified prior to the start of the assessment phase. The Assessment Team requires that application-specific user accounts be created for Assessment Team members, as authorized by the <System Acronym> team. This will enable the Assessment Team to test application security controls and environment vulnerabilities.

Test account creation must be completed no later than two weeks prior to the start of the assessment phase so that the Assessment Team can verify that the test accounts work properly.

Active testing of the application components will be performed in the Implementation environment, while passive review of the configuration of the various database, operating system, and network components will be performed in the Production environment. Based on the defined assessment scope, the application roles and responsibilities/privileges are listed in the following tables.

Table 8. User Roles and Access Privileges

| **System** | **Application** | **Role** | **Privileges** | **Description** |
| --- | --- | --- | --- | --- |
| PRODDB01 | BackupMaster | Administrator | Read, write, and execute for all application data | Administers access control and security functions for the application |
| PRODDB01 | BackupMaster | Supervisor | Read, write, and execute for all application data within their role | Validates or reviews all user application input |
| PRODDB01 | BackupMaster | User | Read all application data within their role | Reads and searches application data |

### Access Mechanisms/Locations

The system’s URLs/IPs are:

* Production: <https://tst-prod.mitre.org/>
* Validation: <https://tst-val.mitre.org/>
* Test: <https://tst-test.mitre.org/>
* Development: <https://tst-dev.mitre.org/>

List and describe any other specific software, thin clients, or utilities required to test the application.

The Assessment Team Lead will inform the System Team when application testing is complete. Following testing, the System Team is expected to initiate the process to de-allocate the security access provided to the Assessment Team test accounts.

## Assumptions/Limitations

The following are assumptions and/or limitations that could affect the Security Assessment:

* Hardware, Networking, Operating System, and Infrastructure components meet the security requirements for a <FIPS 199 Security Level> System.
* The environment and all external systems meet or exceed availability and performance requirements.
* External systems managing sensitive data have an existing Authority to Operate (ATO) and are rated at a Moderate system security level or above.
* Assessment Team personnel will have access to all required components within the system.
* The Assessment Team will have access to all relevant documentation for the system.
* The System Team will be available for support during the assessment.
* The System Team will provide the Assessment Team with accurate information and evidence at all times.
* Information requested by the Assessment Team will be delivered in a timely manner.
* All persons involved in the interview process will be available during their designated interview time.
* The application under test shall be completely free of defects or incomplete code that would prevent the application security tester from proceeding through the application in a manner consistent with an actual user experience.
* No code changes, hot fixes, etc. will be deployed to the assessed environment during the period of the ACT Security Assessment, unless otherwise approved by the Assessment Team.
* Any non-production environments used for assessment purposes will be an exact replica of the production environment; any differences will be clearly and completely explained and documented for the Assessment Team prior to the assessment.
* Test accounts will be tested and made available for every role within the application prior to the first day of testing.
* The Assessment Team will not conduct any testing which requires viewing or obtaining sensitive data such as Personally Identifiable Information (PII), Protected Health Information, (PHI) and/or Federal Tax Information (FTI) data.
* Artifacts provided by the System Team to the Assessment Team will not contain PII, PHI and/or FTI data.
* Assessment Team personnel will have adequate access to the assessment environment(s) between the hours of <Daily Testing Start Time> and <Daily Testing End Time>, and to all required components within the scope of the assessment.
* Assessment of remediation evidence for findings documented in previous assessments is considered to be secondary activity and will be performed only if time and resources permit.

## Points of Contact & Assessment Roles

The Assessment Team points of contact for the ACT Security Assessment are listed in Table 9.

Table . Assessment Team Points of Contact and Roles

| **Role** | **Name** | **Phone Number** | **Email Address** |
| --- | --- | --- | --- |
| Security Assessment Lead |  |  |  |
| M&O Assessor |  |  |  |
| Application Assessor |  |  |  |
| Application Assessor |  |  |  |
| DB Assessor |  |  |  |
| OS Assessor |  |  |  |
| Network Assessor |  |  |  |
| Mainframe Assessor |  |  |  |
| Privacy Assessor |  |  |  |
| Cloud Assessor |  |  |  |
| Virtualization Assessor |  |  |  |

During assessments, testing problems might be encountered and require that System Team personnel be contacted. The points of contact for the ACT Security Assessment are listed in Table 10.

List all <Organization> and Contractor personnel points of contact for this assessment in the table below. Delete rows for roles that are not applicable, and add rows for other applicable rows.

Table . System Team Points of Contact and Roles

| **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 |  |  |  |  |

# Requirements and Schedule

## Physical Access and Work Area Requirements

The Assessment Team will require physical access to various systems, networks, infrastructure, and facilities. The Assessment Team will require direct network connectivity to access applications and Internet access to research findings. For scans, the Assessment Team should be able to connect directly to the switch supporting the network segment that is being assessed, or as close thereto as possible. A work area must be established and include power, table, and chairs.

OR:

The Assessment Team will work remotely – no physical access to systems or facilities will be required.

## Artifact Requirements

The Assessment Team must obtain requested artifacts in a timely manner to avoid delays and improperly reported findings. To effectively perform the assessment and have no delays in the process, the Assessment Team must receive the following system-related artifacts prior to the start of the assessment phase. Failure to receive this information in a timely manner will impact the assessment’s quality and the Assessment Team’s ability to determine whether management, operational, and technical controls have been implemented properly, and may lead to the reporting of incorrect findings. Delivered artifacts should be tagged with the relevant unique Artifact ID from the tables below by prepending the filename with the Artifact ID.

### Tier 1 Artifacts – Minimum Security Artifacts

These artifacts must be provided for use in the development of the Assessment Plan. These artifacts are extremely helpful in determining the system authorization boundary, devices in scope, number of components, system complexity, etc.

Table . Tier 1 Artifacts – Minimum Security Documentation

| **Artifact ID** | **Document/Information Requested** | **Received? (or reason not received)** |
| --- | --- | --- |
| A1-01 | System Security Plan (SSP)  SSP approval / certification evidence |  |
| A1-02 | Information System Risk Assessment (ISRA). |  |
| A1-03 | Contingency Plan (CP). This includes:   * Facility and telecommunications failover * Fail-back planning * CP approval / certification evidence |  |
| A1-04 | Evidence of Contingency Plan Testing.  Include last two (2) tests. |  |
| A1-05 | Detailed network diagram including IP addresses of devices. |  |
| A1-06 | Hardware and software inventories. |  |
| A1-07 | Privacy Impact Assessment (PIA). |  |
| A1-08 | List of ***open system*** POA&Ms[[1]](#footnote-2). |  |
| A1-09 | Specific and detailed access information for all applications and components within scope of assessment (if not documented in the SSP). Examples:   * Uniform Resource Locators (URLs) for web applications * Hostnames, ports, protocols, etc. for console applications |  |
| A1-10 | List of ***open inherited*** POA&Ms. |  |

### Tier 2 Artifacts – Supporting Artifacts

The Tier 2 Artifacts enable the Assessment Team to fully prepare for the upcoming assessment by reviewing all system documentation, baseline configurations, and process evidence prior to the formal assessment period. If the provided artifacts do not fully meet the information request, the Assessment Team will identify such gaps to the System Team so that they can quickly retrieve and provide the additional information.

Customize the table below based on the scope of the assessment. Remove any artifacts not within scope – do not adjust Artifact ID #s.>

Table . Tier 2 Artifacts – Supporting Artifacts

| **Artifact ID** | **Document/Information Requested** | **Received? (or reason not received)** |
| --- | --- | --- |
| A2-01 | Risk Acceptance letters. |  |
| A2-02 | Process documentation for vulnerability scanning (to include scan configuration, result review, and remediation). |  |
| A2-03 | Evidence of the most recent vulnerability scan results of the infrastructure in scope (using whichever tool that the system relies upon in their review process). |  |
| A2-04 | Updated list of ***open*** Plan of Action and Milestones (POA&M) (if changed since submission as part of Tier 1 Artifacts). |  |
| A2-05 | Technical Review Board (TRB) and Technical Reference Architecture (TRA) letters and related documentation.  Primarily for major updates and new applications. |  |
| A2-06 | Configuration and change management process documentation. Include:   * examples of Change Requests (CR) from request to implementation in production * list of change control board members * emergency change procedures * change validation procedures |  |
| A2-07 | The ***implemented*** baseline security configurations (e.g., United States Government Configuration Baseline [USGCB], Secure Technical Implementation Guide [STIG], etc.) for each infrastructure component device (Windows, Linux, IOS, Solaris, mainframe, etc.) within this system’s Authorization Boundary. |  |
| A2-08 | Process documentation that describes the methods used for configuration policy compliance audits for each of the infrastructure components (to include validation frequency, review processes, and violation response). |  |
| A2-09 | Process documentation describing how exceptions to baseline configurations are approved and a listing of exceptions for each infrastructure component device in scope (if not provided in the implemented baseline evidence). |  |
| A2-10 | Evidence of most recent configuration baseline policy compliance audits/scans of the infrastructure within scope. |  |
| A2-11 | Process documentation for maintenance, update, and validation of the Information System Component Inventory (to include how rogue devices are identified, new devices are added, and frequency of the revalidation). |  |
| A2-12 | Compliance monitoring tool output (*e.g.*, Nessus, nCircle, *etc.*). |  |
| A2-13 | Process documentation for patch application for each of the infrastructure components (to include platform, schedule, testing process). |  |
| A2-14 | Malware protection process documentation (to include ruleset update frequency, scan frequency, and alert management). |  |
| A2-15 | Process documentation regarding how host information integrity is maintained (to include intrusion detection monitoring, maintenance, and response). |  |
| A2-16 | For each infrastructure component device (Windows, Linux, IOS, Solaris, mainframe, etc.) within scope, documentation describing UserID conventions such as:   * Account naming conventions, defined groups (Administrator, User, Contractor, etc.), and conditions for group membership * Processes and tools used for monitoring adherence to account management and password directives |  |
| A2-17 | For each infrastructure component device (Windows, Linux, IOS, Solaris, mainframe, etc.) within scope, evidence that reflects information system accounts and group membership are reviewed and certified. |  |
| A2-18 | Documentation describing the types of audit logging that the system implements in support of organizational policies.  Should describe how each information system component (i.e., for each component type listed in the system inventory) is configured to record relevant audit records (e.g., syslog for Unix, SMF for mainframe).  Should define the information system’s audit requirements (e.g., failed login attempts). |  |
| A2-19 | * Process/procedure documentation that describes how audit records are securely stored/protected and ensures no loss of data due to processing failures.   Should describe the specific technologies utilized to either prevent or alert staff when a failure occurs or is pending (due to storage issues etc.). |  |
| A2-20 | Documentation describing the established rules for log review and analysis, and reporting (to include Security Information and Event Management [SIEM]).  Should describe the ruleset used by the SIEM with an emphasis on the criteria, by type (low, medium, high), that must be met to alert a SIEM admin.  Should describe the procedures/process for handling low, med, high event (e.g., timeframes for escalation into the incident response process. |  |
| A2-21 | Process/procedure documentation that describes how audit information is protected from unauthorized access (read and update) and non-repudiation mechanisms.  Should describe both the tool protections specifically employed as well as non-tool access (e.g., if a database/data store is used, how is this data protected from direct access for read/update).  Should describe which information system components have implemented non-repudiation services and the associated actions under protection; description should explain the technologies used to deploy the non-repudiation service. |  |
| A2-22 | System Design Document (SDD). |  |
| A2-23 | System backup and storage requirements and procedures. |  |
| A2-24 | Rules of Behavior (ROB). |  |
| A2-25 | Procedures describing processes in place for security-related activity planning of the information system. |  |
| A2-26 | Incident Response policy, plan and process documentation. Include:   * description of incident response teams and responsibilities * list of staff on incident response teams * analysis processes to identify incidents * reporting procedures * tools used in support of the incident management function * examples of tracking tickets for incidents that were identified, reviewed, and closed |  |
| A2-27 | Incident Response training, testing and exercise material. |  |
| A2-28 | Job descriptions, position requirements, sensitivity levels, etc. for key organizational positions including:   * ISSO/ISSM * security analysts and administrators * system administrators * network administrators * database administrators |  |
| A2-29 | Personnel policies and procedures that address:   * personnel screening requirements * personnel hiring, transfers, and terminations * access agreements or expected rules of behavior * sanctions for non-compliance to information security policies and procedures |  |
| A2-30 | Procedures and requirements for contractors or non-organizational entities that provide services or support to the environment. |  |
| A2-31 | Physical access policies and procedures describing the processes and tools for:   * granting access to the facility and datacenter * authorizing, reviewing, and deleting individual access to the datacenter |  |
| A2-32 | Inventory procedures that describe the processes for adding, monitoring (inventorying), and decommissioning equipment purchased in support of the organization. |  |
| A2-33 | Policies and procedures that describe the requirements and expectations for employees supporting the organization and working remotely (i.e., safeguarding equipment, reporting security incidents, etc.). |  |
| A2-34 | Source code. **NOTE: Only provide if assessment of source code is specifically requested**. |  |
| A2-35 | Security awareness and role-based training materials used to train system personnel.  Training slides, handouts, etc. |  |
| A2-36 | Evidence that security awareness and role-based training has been completed by system personnel.  Training certificates, attendance sheets, etc. |  |
| A2-37 | Evidence that Rules of Behavior (RoBs) have been acknowledged/signed by users. |  |
| A2-38 | System of Record Notice (SORN). |  |
| A2-39 | CP recovery priority list (business functions, applications, IT infrastructure). |  |
| A2-40 | Incident Response training, testing, and exercise attendance records for the past two (2) years (sampling is acceptable). |  |
| A2-41 | Personnel and/or security records that reflect:   * personnel were screened prior to hire and transfers * upon termination, exit interviews were conducted, information system and facility access were disabled * information system and physical access authorizations were reviewed and updated for personnel who transferred position * signed or acknowledged access agreements (for past two (2) years – sampling is fine)   *Note: the records may be reviewed (shoulder surfing) or names removed from provided output.* |  |
| A2-42 | Physical authorization to the datacenter including:   * list of individuals authorized * evidence of past five (5) reviews of the list identifying those authorized to the datacenter * supporting documentation from adding and deleting access for several individuals * evidence of the past five (5) reviews logs depicting physical access to the datacenter |  |
| A2-43 | Visitor access logs to the facility from two (2) days. *Note: the logs may be reviewed by the assessor in-person vs. generating a copy (i.e., “shoulder surfing”)*. |  |

## Technical Output Artifacts

Customize this section based on the scope of the assessment.

The Assessment Team will examine technical data to determine whether the system correctly implements documented baselines, generates appropriate audit records, enforces appropriate password policies, monitors local administrator accounts, etc. Output from tools currently used across the Organization’s enterprise (such as InSpec) must be provided (if applicable), and the Assessment Team may provide additional scripts, tools, and/or other information requests for the System Team to execute and return to the Assessment Team. ***The Assessment Team must obtain the requested technical output no later than two weeks prior to the assessment Kick-off meeting, unless otherwise agreed by the System Team and the Assessment Team.***

*Note: Failure to provide the technical output to the Assessment Team within the required timeframe will negatively impact the assessment’s quality and the Assessment Team’s ability to determine whether security controls have been implemented properly.*

Table . Technical Output Artifacts

| **Artifact ID** | **Document/Information Requested** | **Received? (& reason not received)** |
| --- | --- | --- |
| TO-CL | Cloud technology technical output. Includes output from cloud platforms and technologies such as Amazon AWS, Microsoft Azure, custom data collection scripts provided by the Assessment Team, *etc*. |  |
| TO-DB | Database technical output. Includes output from tools such as DbProtect, InSpec, Nessus, custom data collection scripts provided by the Assessment Team, *etc.* |  |
| TO-MA | Mainframe security configuration data (RACF, *etc.*). |  |
| TO-NT | Network device(s) technical output. Includes running configuration(s), output from tools such as InSpec, Nessus, custom data collection scripts provided by the Assessment Team, *etc.* |  |
| TO-OS | Operating System(s) technical output. Includes output from tools such as InSpec, Nessus, custom data collection scripts provided by the Assessment Team, *etc.* |  |
| TO-VI | Virtualization technology technical output. Includes output from tools such as VMware, Citrix, custom data collection scripts provided by the Assessment Team, *etc.* |  |

## Security Assessment Schedule

Customize this section based on the scope of the assessment.

System Team personnel will need to be available during the assessment period in order to improve the assessment’s efficiency and accuracy. The interactions with the Assessment Team may include technical consultation; supervised access to systems, networks, infrastructures, or facilities; and monitoring of assessment activities. The following rough schedule outlines anticipated staff requirements:

Table . ACT Security Assessment Schedule

| **Monday** | **Tuesday** | **Wednesday** | **Thursday** | **Friday** |
| --- | --- | --- | --- | --- |
| Arrive onsite at 8:30 a.m. (Local) | Arrive onsite at 8:30 a.m. (Local) | Arrive onsite at 8:30 a.m. (Local) | Arrive onsite at 8:30 a.m. (Local) | Arrive onsite at 8:30 a.m. (Local) |
| Set up workspace and establish procedures for network connection. | Privacy SME Interview | Application Developer Interview | Windows System Admin Interview |  |
| Conduct “Kick-off” meeting and system walk through. | Contingency / Disaster Recovery Manager Interview | Network Admin Interview | Linux System Admin Interview |  |
| Datacenter / Facilities Tour | Configuration Manager Interview | Database Admin Interview | Security Utilities and Firewall Admin Interview (Incident Response) |  |
| ISSO/Business Owner Interview | Cloud Admin Interview | Mainframe System Admin Interview | Documentation Review with ISSO/ISSM  Meeting with the Business Owners and provide feedback on SSP, ISRA and CP documents. |  |
| Training Manager / Human Resources Representative Interview | Virtualization Admin Interview |  |  |  |
| Perform application testing. | Perform application testing. | Perform application testing. | Perform application testing. | Complete application testing. |
| Perform network-based scanning of all Web servers and interfaces. | Perform network-based scanning of all Web servers and interfaces. | Perform network-based scanning of all Web servers and interfaces. | Perform network-based scanning of all Web servers and interfaces. | Testing and Interviews (as needed). |
|  | Conduct Daily Update (as needed). | Conduct Daily Update (as needed). | Conduct Daily Update (as needed). | Conduct Daily Update (as needed) or Final Update. |

## Security Assessment Estimated Timeline

The following table describes the estimated timeline for assessment actions and milestones.

Table . Estimated Timeline for Security Assessment Actions and Milestones

| **Action/Milestone** | **Description** | **Date(s)** |
| --- | --- | --- |
| Perform Readiness Review | Discuss assessment preparations and ensure tasks (*e.g.,* account creation and providing documentation to the Assessment Team) are on target for completion. | <ACT Lead schedules one to two weeks prior to ACT> |
| Establish and test accounts | Set up and test all test accounts for the assessment. |  |
| Deliver documentation, script output, and configuration output to the Assessment Team | Deliver all documentation, script output, and configuration data to the Assessment Team prior to assessment. |  |
| Perform Assessment | Conduct technical testing and Management and Operations interviews based on the assessment’s scope. |  |
| Conduct Final Update (if needed) | Review and summarize security vulnerabilities from assessment. |  |
| Remove security access | ISSO/ISSM removes security access established for Assessment Team test accounts. |  |
| Deliver ACT Security Assessment Report to System Team | Put security vulnerabilities identified during the assessment into report format. |  |
| Conduct Review of Report | System personnel and Assessment Team meet to review feedback on Draft Report. System personnel should provide feedback to Assessment Team prior to meeting. |  |
| Deliver updated ACT Security Assessment Report and Findings Spreadsheet to System Team | Updated based on system team feedback. |  |
| Deliver Final Package to System Team | Contains all deliverables, work products, artifacts, etc. |  |

# ACT Security Assessment Process and Methodology

This section outlines the Assessment Team’s assessment methodology to verify and validate that the information system’s Security Capabilities are appropriately implemented via assessment of management, operational, and technical controls.

## Assessment Phases

The ACT Security Assessment process is generally executed using a phased approached described below.

### Phase 1: Planning

Phase 1, *“Planning”,* defines the assessment’s scope, identifies goals, sets boundaries, and identifies assessment activities. This phase, as well as subsequent phases, requires the coordination of all involved parties, including: system ISSO/ISSM and Business Owner, <Organization> InfoSec, the Assessment Team, and the System Team.

During this phase, the Assessment Team works with the ISSO/ISSM and Business Owner to determine the scope of the ACT, including:

* Which **Capabilities and Sub-Capabilities** should be included in the assessment, and which should receive the most emphasis.
* Which **security controls** should be included in the assessment, and which should receive the most emphasis.
  + *Note that the* ***<Organization> Core Controls*** *are always in-scope and receive emphasis unless otherwise noted in the ACT Security Assessment Plan.*
* Which system components (software or hardware) should be included in the assessment, and which should receive the most emphasis.

The Assessment Team will then define agreeable assessment terms and create the Security Assessment Plan (this document). The System Team and any other appropriate parties will review and provide feedback on the Security Assessment Plan. The Assessment Team will then update and publish the final version of the Security Assessment Plan.

### Phase 2: Assessment

Phase 2, “*Assessment*”, may have several steps depending on the assessment’s objectives, scope, and goals, as set forth in the Planning Phase. These steps can be grouped by the nature of the activities involved. These activity groups are as follows:

* Which **Capabilities and Sub-Capabilities** should be included in the assessment, and which should receive the most emphasis.
* **Enumeration:** activities that provide specific information about assessment targets. This information is often collected using appropriate software tools.
* **Core Controls Testing and Review:** Assessment of the <Organization> Core Controls was emphasized as part of this ACT. Each Core Control is rigorously assessed against at least the relevant Test Methods listed in the relevant security controls catalog.
* **Other Testing and Review:** activities that typically involve the automated testing of security vulnerabilities software tools, manual analysis, and the evaluation of the System Security Plan (SSP) and particular aspects of the organization’s security policies and practices by the Assessment Team members. Existing penetration test results, if available, are also typically reviewed. The Assessment Team applies experience and insight in order to determine whether the system adequately implements the <Organization> Core Controls and other in-scope security controls and Capabilities/Sub-Capabilities defined by Organizational policies and standards, and whether known vulnerabilities are mitigated.

### Phase 3: Reporting

Phase 3, “Reporting”, documents the soundness of the implemented security controls and consolidates all findings into the final output. This output includes reports that provide a summary of key findings and actionable recommendations, as well as provisions for all information derived from the assessment.

Depending on the results of these activities, it may be necessary to repeat parts of some phases. Throughout the entire process, the Assessment Team will keep all involved parties informed of the progress and findings, as well as provide briefings of findings to System Team personnel. Evidence to support any weaknesses discovered will consist primarily of screen prints, script or analysis tool output, and session data. The Assessment Team will immediately notify System Team personnel if significant or immediately exploitable vulnerabilities are discovered during the assessment.

## Roles and Responsibilities

To prepare for the assessment, the System Team and the Assessment Team will identify personnel associated with specific responsibilities. Individuals may have responsibilities that span multiple roles, or have knowledge pertaining to the implementation of more than one security control area. This section provides a description of the roles and responsibilities to assist the organization(s) and the Assessment Team in determining the appropriate personnel who should be available for the assessment.

Customize the roles based on the assessment’s scope. Not all roles may exist/apply.

### Application Developer/Maintainer

The Application Developer/Maintainer shall have a thorough knowledge of the application security control requirements for the system and their implementation to protect the software application, its data in transit and at rest, as well as the implementation and configuration standards utilized by the organization. These controls may include; access control, audit and accountability, user identification and authentication, software code configuration control, application integrity, and communications protection. During the ACT process, the Application Developer/Maintainer shall be available for planning sessions, interviews, application discussions, providing assistance for using the application, providing documentation under their control, and remediating any weaknesses.

### Security Assessment Lead

The Security Assessment Lead is a member of the Assessment Team and responsible for understanding <Organization> policies, standards, procedures, system architecture, and structures. The Security Assessment Lead has limited activities within the ACT scope; reports all vulnerabilities that may impact the overall security posture of the system; and coordinates getting information, documentation and/or issues addressed between the Assessment Team and the System Team. The Security Assessment Lead must develop the Security Assessment Plan; modify the testing approach, when necessary according to the scope of the assessment; prepare the daily agenda, preliminary findings worksheets, and conduct the Assessment briefings; and prepare an ACT Security Assessment Report to communicate how the <Organization> business mission will be impacted if an identified vulnerability is exploited. The Security Assessment Lead is responsible for all administrative and management tasks for the Security Assessment.

### Business Owner

The Business Owner is responsible for the successful operation of the system and is ultimately accountable for system security. The Business Owner defines the system’s functional requirements, ensures that Assessment and Authorization (A&A) activities are completed, maintains and reports on the Plan of Action & Milestones (POA&M), and ensures that resources necessary for a smooth assessment are made available to the Assessment Team (Assessment Contractor). During the ACT process, the Business Owner shall be available for planning sessions, interviews, system discussions, providing documentation, and providing assistance when necessary (access, contacts, decisions, etc.). In some cases, the Business Owner may be the System Owner.

### Configuration Manager

The Configuration Manager shall be able to describe the policy, processes, procedures, standards, and technical measures utilized for configuration management and change control, in order to maintain a secure system baseline. The Configuration Manager shall be able to provide details of the application specific or system/enterprise configuration/change control processes and documentation, including identification, configuration/change management plan, status accounting, and audit procedures. The baseline could include, but is not limited to; software configuration, network infrastructure configuration, and, application design and development resources. During the ACT process, the Configuration Manager shall be available for interviews, and to provide documentation under the Configuration Manager’s responsibility.

### Contingency Planning Manager

The Contingency Planning Manager develops the Contingency Plan for system recovery, and works with the Business Owner and System Owner to determine the critical components and an appropriate system recovery strategy based on the business impact analysis, system Recovery Time Objective (RTO), and Recovery Point Objectives (RPO). The Contingency Planning Manager develops and maintains the Contingency Plan for the system, ensuring that testing of the plan is completed based on the organizational and business requirements. During the ACT process, the Contingency Planning Manager shall be available for interviews and to provide the System Contingency Plan documentation and update process, system contingency testing schedule, and system contingency plan test reports.

### Database Administrator

The Database Administrator(s) shall have a thorough knowledge of the database software and the databases that support the system, as well as the implementation and configuration standards utilized by the organization for the software and databases. The Database Administrator shall be able to describe the processes and procedures for installing, supporting, and maintaining the database software and databases, including; secure baseline installation, access control, identification and authentication, backup and restoration, and flaw remediation. During the ACT process, the Database Administrator shall be available for interview, database discussions, execution of scripts to collect configuration details, providing documentation when necessary, and remediation of any weaknesses.

### Datacenter / Facilities Manager

The Datacenter/Facilities Manager may have multiple responsibilities, including the development of physical and environmental control policies for the datacenter and ensuring policy compliance. The Datacenter/Facilities Manager should be able to describe the physical and environmental (e.g., power, fire suppression, cooling/heating) controls that help secure the system, data, and contingency plans for the datacenter. In some instances, the Datacenter/Facilities Manager may be responsible for system media protection controls as media enters or departs the facility. During the assessment, the Datacenter/Facilities Manager should be available for interview, and to provide documentation related to controls under the Datacenter/Facilities Manager’s responsibility.

### Development Lead

The Development Lead is responsible for implementing the design and requirements of the system’s various design and specification documents. The Development Lead may also be responsible for assisting <Organization> with determining the design and functional requirements of the system.

### Firewall Administrator

The Firewall Administrator(s) should have an intimate knowledge of the firewalls supporting the system, as well as the implementation and configuration standards utilized by the organization. The Firewall Administrator(s) should have an in-depth knowledge of the boundary and segment isolation mechanisms, including; firewall servers, appliances, and integrated access control devices. This role may be combined with the Network Administrator role. During the assessment, the Firewall Administrator should provide firewall rules, and be available for interview, firewall discussions, execution of scripts to collect configuration details, and remediation of any weaknesses found that could be corrected within the assessment timeframe.

### Human Resources Manager

Human Resources (HR) staff should have an understanding of the organization’s personnel policies, with an impact on information technology security and their implementation for the organization. This would include; policies and procedures related to background investigations, hiring practices, personnel classifications, training requirements, terminations, and transfers.

### Incident Handling Manager

The Incident Handling Manager oversees the organization’s information system incident management function and should have an understanding of how incidents are identified, analyzed, assessed to determine the security incident’s impact and priority, and response procedures.

### Information System Security Manager

The Information System Security Manager (ISSM) is responsible for the information assurance of a program, organization, system(s), or enclave. Can also be responsible for the management of ISSOs.

### Information System Security Officer or Information System Security Manager

The Information System Security Officer (ISSO) or Information System Security Manager (ISSM), is responsible for ensuring that the management, operational, and technical controls to secure the system are in place and effective. The ISSO/ISSM shall have knowledge of the following:

* All controls implemented or planned for the system
* Security audit controls and evidence that audit reviews occur
* System Security Plan (SSP) and any authorized exceptions to security control implementations

The ISSO/ISSM shall be responsible for all security aspects of the system from its inception, until disposal. During the ACT process, the ISSO/ISSM plays an active role and partners with the <Organization> Facilitator to ensure a successful ACT. The ISSO/ISSM shall be available for interview, provide or coordinate the timely delivery of all required ACT documentation; and coordinate and schedule interviews between the Assessment Team and ACT Stakeholders. The ISSO/ISSM is designated in writing, must be a <Organization> employee, and can be a System Developer/System Maintainer ISSO.

### Mainframe Administrator

The Mainframe Administrator(s) should have knowledge of the mainframe hardware and software supporting the system, as well as the implementation and configuration standards utilized by the organization for the system. The Mainframe Administrator should be able to describe the processes and procedures for installing, supporting, and maintaining the mainframe, including; secure baseline installation, access control, identification and authentication, backup and restoration, and flaw remediation. During the assessment, the Mainframe Administrator should be able to provide information about the mainframe and implemented security controls, as well as be available for interview, mainframe discussions, execution of scripts to collect configuration details, and remediation of any weaknesses found that could be corrected within the assessment timeframe.

### Media Custodian

The Media Custodian is responsible for ensuring system media protection, which includes; labeling, marking, and transporting both electronic and paper media for the system. During the assessment, the Media Custodian should be available for interview and to provide evidence of implemented media protection controls.

### Middleware Utilities Administrator

The Middleware Utilities Administrator(s) should have a thorough knowledge of the system middleware utilities implemented in the infrastructure. The Middleware Utilities Administrator should be able to describe the processes and procedures for installing, supporting, and maintaining the middleware utilities, including; any secure baseline installation, access control, identification and authentication, backup and restoration, and flaw remediation. During the assessment, the Middleware Utilities Administrator should be able to provide information for implemented middleware utilities and access to the utilities, as well as be available for interview, utilities discussions, execution of scripts to collect configuration details, and remediation of any weaknesses found that could be corrected within the assessment timeframe.

### Network Administrator

The Network Administrator(s) should have a strong knowledge of the underlying network infrastructure and architecture that supports the system, as well as the implementation and configuration standards utilized by the organization. Depending on the organization and/or system, Network Administrators may provide; network address assignments, routing protocol assignments and routing table configurations, Virtual Local Area Network (VLAN) implementation, and network device configuration. Their role could also include; configuration of authentication and authorization, directory services, printers, Virtual Private Network (VPN) gateways, load balancers, and other network services. If the Network Administrator has security-related duties, he/she may be responsible for firewall implementation and management, intrusion detection systems, and security event monitoring. During the assessment, the Network Administrator should be available to establish network access, interview, network discussions, execution of scripts to collect configuration details, and remediation of any weaknesses found that could be corrected within the assessment timeframe.

### Privacy Subject Matter Expert

The Privacy Subject Matter Expert (PSME) provides guidance in the development, implementation, and maintenance of the system’s information privacy policies and procedures, ensuring that they comply with higher-level organizational requirements. During the ACT process, the PSME shall be available for interview and provide documentation that falls under the PSME’s responsibility.

### Program Manager

The Program Manager shall have a high-level understanding of the assessed system, as well as the ability to describe organizational and system policies from an enterprise perspective, with which the system shall be in compliance. The Program Manager shall be familiar with; access controls (both physical and logical), contingency plans (i.e., alternate sites/storage, system restoration and reconstitution), user identification and authentication, system authorization to operate, incident response, resource planning, system and software acquisition, flaw remediation, and system interconnections and monitoring. During the ACT process, the Program Manager shall be available for interview and to provide documentation that falls under the Program Manager’s responsibility.

### Security Utilities Administrator

The Security Utilities Administrator(s) should have a thorough knowledge of the system security utilities, such as intrusion detection systems/prevention or security event monitoring, that is implemented in the infrastructure. The Security Utilities Administrator should be able to describe the processes and procedures for installing, supporting, and maintaining the utilities, including; any secure baseline installation, access control, identification and authentication, backup and restoration, and flaw remediation. During the assessment, the Security Utilities Administrator should be able to provide information on the utilities in place and access to those utilities, as well as for interview, utilities discussions, execution of scripts to collect configuration details, and remediation of any weaknesses found that can be corrected within the assessment timeframe.

### System Administrator

The System Administrator(s) should have a thorough knowledge of the operating systems for which they are responsible, as well as the implementation and configuration standards utilized by the organization for those operating systems. The System Administrator(s) should be able to describe the processes and procedures for installing, supporting, and maintaining the operating systems, including; secure baseline installation, access control, identification and authentication, backup and restoration, flaw remediation, and use of antivirus products. During the assessment, the System Administrator(s) should be available to; establish access to the system, interview, system discussions, execution of scripts to collect configuration details, and remediation of any weaknesses found that could be corrected within the assessment timeframe.

### System Owner

The System Owner is responsible for the successful operation of the system and accountable for system security. The System Owner is also responsible for executing crucial steps to implement management and operational controls, and to ensure that effective technical controls are implemented to protect the system and its data. The System Owner formally designates the ISSO. In conjunction with the Business Owner, the System Owner is responsible for ensuring that Security Accreditation activities are completed, and that the POA&M is maintained and reported. During the ACT process, the System Owner shall be available for interview and, with the assistance of the system’s support staff, ensure that all documentation required for the assessment is available to the ACT Evaluator. The System Owner may be the Business Owner.

### Training Manager

The Training Manager is responsible for ensuring that all system users receive security awareness training, and for providing role-based training support for staff with information security specific roles. The Training Manager is responsible for maintaining security training records for all system users. During the assessment, the Training Manager should be available for interview, and to provide documentation for the awareness training, security role training, and training completion evidence.

## Security Assessment Activities

The Assessment Team will assess whether Security Capabilities are being implemented by performing activities that typically involve both the automated testing of security vulnerabilities via software tools, manual analysis, and the evaluation of particular aspects of the organization’s security policies and practices.

### Level of Testing Rigor

Since the goal of a Security Assessment is to determine both the system’s *actual* compliance with the Security Controls *and* the *correctness* and *reliability* of the system’s Security Control compliance *assertions*, <Organization> must specify how much assurance they require. ACT specifies four different *Testing Rigor Levels* that provide increasing levels of assurance that the assertions made in documentation and interviews are correct and that the system correctly implements and complies with <Organization>’s security controls catalog. These Levels are described in the table below:

Table 16. Levels of Testing Rigor



The Assessment Team must tailor their assessment methods to meet the verification objectives of the Level of Testing Rigor that is specified for the Security Assessment. **The default Level of Testing Rigor for each Security Assessment is Level 3 “Basic Compliance Verification”**, but the Authorizing Official or System Team may choose to specify a different Level of Testing Rigor if appropriate. At Level 3, the Security Assessment Lead must work with the System Team to determine what type of sampling of the Non-Core Controls’ assertions is acceptable. **For this Security Assessment, the System Team has chosen Testing Rigor Level <Testing Rigor Level>.**

### Documentation Review

Prior to and during the assessment phase, the Assessment Team will review documents provided by the System Team. The review will assess whether appropriate management and operational controls have been implemented. However, it will also be used to augment technical controls. For example, if the security control catalog stipulates that the password length for the information system is required to be eight characters, and the SSP documents that the length of passwords is eight characters, the technical assessment will confirm whether passwords are configured to be eight characters in length.

Unless otherwise noted, the ACT will always involve full assessment of the SSP document (including all controls, both in-scope and out-of-scope, since it is not possible to determine whether the SSP is adequate without understanding each control response in-context with the others). The ACT will also assess the Information System Risk Assessment (ISRA), Contingency Plan (CP), and Privacy Impact Assessment (PIA) if the relevant Capabilities or Security Controls are in scope.

### Application Testing

Customize this section based on the act’s scope and the testing environment.

The Assessment Team will test the system to assess whether Security Capabilities and Security Controls are being implemented through proper software development techniques, supported software is used, and that the Confidentiality, Integrity, and Availability (CIA) of data processed by the application adheres to applicable Organizational policies, procedures, and standards. The application testing will include what is commonly called “Vulnerability Assessment”, and it is common to encounter confusion about the difference between Vulnerability Assessment and Penetration Testing (which is one of the RIS used in the ACT Risk Assessment). For purposes of the ACT Security Assessment, a Vulnerability Assessment looks for vulnerabilities in a system and reports potential exposures, while a Penetration Test exploits vulnerabilities and other weaknesses in the architecture of the system or network to determine the degree to which a malicious attacker can gain unauthorized access to the system. However, the Vulnerability Assessment stops once a determination is made that a vulnerability could (or could likely) be exploited – the Assessors will not attempt to fully exploit and escalate the vulnerabilities (as a Penetration Test would).

The following is a non-comprehensive list of activities the Assessment Team might perform:

* Assess if input parameters passed to the application are checked and validated
* Determine if application administrators can remotely access the application via Organization-approved standards
* Examine implemented access control, and identification and authentication techniques
* Test to determine if the application is susceptible to Cross-Site Scripting (XSS), Structured Query Language (SQL) injection, or other vulnerabilities
* Examine confidential information to determine if it is encrypted before being passed between the application and browser
* Determine if the application architecture conforms to the Organization’s defined Technical Reference Architecture (TRA)

The System Team will provide the appropriate user accounts and logins to access the application to be tested in the targeted environment. The user account logins and application access must be available to the Assessment Team for tests, two weeks prior to application testing. At least one account must have administrative access with the ability to adjust the application roles of another login.

#### Potential Assessment Tools

The Assessment Team will work with the System Team to ensure that industry best practices are reflected in the system’s architecture and design. Tools used by the team during the assessment may include (but are not limited to):

Table . Potential Assessment Tools (Non-Comprehensive)

| Tool Name | Description |
| --- | --- |
| [Aqua](https://www.aquasec.com/) | Security scanner for cloud native apps & infrastructure: containers, serverless, and VMs, across all platforms and clouds. |
| [Atomic Red Team](https://github.com/redcanaryco/atomic-red-team) | Uses Red Canary scripts (based on the [MITRE ATT&CK](https://attack.mitre.org/) framework) that execute simple "atomic tests" that exercise the same techniques used by adversaries. |
| [Burp Suite](http://portswigger.net/burp/) | Integrated platform for performing security testing of web applications. |
| [Curl](http://curl.haxx.se/) | Open-source command line tool for transferring files with Uniform Resource Locator (URL) syntax. |
| Custom Data Collection Scripts | Developed and maintained by MITRE’s assessment team with the contribution and experience of vulnerability and technical testers. |
| [DbProtect](https://www.trustwave.com/en-us/services/technology/dbprotect/) | Database security platform that uncovers database configuration mistakes, identification and access control issues, missing patches, or any toxic combination of settings that could lead to various types of negative outcomes. |
| [InSpec](http://inspec.io/) | Open-source testing framework for infrastructure with a human- and machine-readable language for specifying compliance, security and policy requirements. |
| [GoBuster](https://github.com/OJ/gobuster) | GoBuster is a tool used to brute-force: URIs (directories and files) in web sites; DNS subdomains (with wildcard support); and Virtual Host names on target web servers. |
| [Maltego](https://www.paterva.com/) | Maltego is an interactive data mining tool that renders directed graphs for link analysis. The tool is used in online investigations for finding relationships between pieces of information from various sources located on the Internet. |
| [Mozilla Firefox Web Browser](http://www.mozilla.org/) | Open-source Web-based browsers used to manually browse and inspect the Web application and associated forms with useful add-ons for exploitation/inspection. |
| [Nessus](http://www.nessus.org/) | Open-source vulnerability scanner and assessment tool. |
| [NetSparker](http://www.netsparker.com/) | Multi-user web security scanner with built-in workflow and reporting tools. |
| [Nmap](https://nmap.org/download.html) | Nmap, short for Network Mapper, is a free, open-source tool for vulnerability scanning and network discovery. Network administrators use Nmap to identify what devices are running on their systems, discovering hosts that are available and the services they offer, finding open ports and detecting security risks. |
| [PowerSploit / PowerView](https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon) | PowerView is a PowerShell tool to gain network situational awareness on Windows domains. It contains a set of pure-PowerShell replacements for various windows "net \*" commands, which utilize PowerShell AD hooks and underlying Win32 API functions to perform useful Windows domain functionality. |
| SCAP Compliance Checker (SCC) & CIS CAT PRO | SCC and CIS CAT PRO allow the comparison of systems against various baseline standards. These include CIS level 1, level 2, and DISA STIGs.  Note: Requires memberships to MAX.gov and CIS for download. |
| [Sn1per](https://github.com/1N3/Sn1per) | Sn1per is an automated scanner that can be used during a penetration test to enumerate and scan for vulnerabilities. Sn1per Professional is Xero Security's premium reporting addon for Professional Penetration Testers, Bug Bounty Researchers and Corporate Security teams to manage large environments and pen test scopes. |
| [Veracode Static Analysis](https://www.veracode.com/products/binary-static-analysis-sast) | Static code analysis tool. Provides automated security feedback in the IDE and the pipeline, and conducts a full policy scan before deployment. It then provides clear guidance on what issues to focus on and how to fix them faster. |
| [W3af](https://github.com/andresriancho/w3af/) | w3af is an open source web application security scanner which helps developers and penetration testers identify and exploit vulnerabilities in their web applications.  The scanner is able to identify 200+ vulnerabilities, including Cross-Site Scripting, SQL injection and OS commanding. |
| [WeirdAAL](https://github.com/carnal0wnage/weirdAAL) | WeirdAAL is an AWS penetration testing framework that allows enumeration of various services such as AWS lambda and IAM based modules. |
| [wget](http://www.gnu.org/software/wget/wget.html) | Open-source network tool that retrieves files from the Internet using HTTP, Secure Hyper Text Transfer Protocol (HTTPS), and the File Transfer Protocol (FTP). |
| [Wireshark](http://www.wireshark.org/) | Open-source, GUI network packet and protocol analyzer. |
| [Zed Attack Proxy (ZAP)](https://www.zaproxy.org/) | Open-source web application scanner. |

### Database Server/Instance Testing

Customize this section based on the scope of the assessment.

The Assessment Team will evaluate database server and software configurations to assess whether Security Capabilities are being implemented with the help of the appropriate system administrators. The Assessment Team technical staff will work with the system administrators and DBAs to view essential, security-relevant configurations and settings. The following is a list of activities that will be performed:

* Review the results of Nessus vulnerability scans to identify known flaws in the <Database type: Oracle, SQL Server, Informix, DB2, M204, MySQL, etc.> server version and settings
* Review database security configuration settings to determine if adequate system protections are implemented
* Interview the system and database administrators concerning database server configurations and security relevant mechanisms

### Interviews

Interviews will focus on a review of the management, operational, and technical controls associated with the in-scope Security Capabilities, Technical Reference Architecture (TRA), security policies, procedures, and standards. Interviews will also help gain a better understanding of the system environment’s security posture and will supplement findings identified during the technical testing. When available and applicable, electronic copies of additional written documentation will be collected for review. Subject Matter Experts (SME) in the following areas might be interviewed:

* System architecture and development methodologies
* System security policies
* Configuration management processes
* Patch management
* Distribution of anti-virus software
* Intrusion Detection/Prevention Systems (IDS/IPS)
* Incident response to intrusion, virus infection, and Denial of Service (DoS)
* Audits and log analysis
* Network/systems monitoring and management
* Contingency planning and backup and recovery
* Mainframe application architecture and implementation pertaining to <System Acronym> operations
* Batch files management processes

### Network Scans

Customize this section based on the scope of the assessment.

The Assessment Team will assess whether Security Capabilities are being implemented by utilizing <Organization> InfoSec-provided network-based scans of all in-scope devices to determine ports, protocols, and services running on each host, and the extent to which the system implementation meets security control requirements. If adequate <Organization> InfoSec-provided data is not available, the Assessment Team will perform their own scans in coordination with the System Team.

#### Network Mapping and Asset Discovery

Note: This section (and activity) is usually required for HVAs (unless otherwise specified by the Authorizing Official or System Team) and is typically not performed for non-HVAs (unless otherwise specified by the Authorizing Official or System Team).

Utilizing automated tools and SOC-provided data, the Assessment Team will scan specific network segments to discover active systems, and the services offered by those systems.

### Penetration Testing

Note: This section (and activity) is required for HVAs (unless otherwise specified by the Authorizing Official or System Team) and is typically not performed for non-HVAs (unless otherwise specified by the Authorizing Official or System Team).

The Assessment Team will [attempt to gain access to the system via typical penetration testing techniques with [full / limited] knowledge of the system] OR [review results of penetration testing performed by <Penetration Test Assessor> on <Date>].

### Wireless Assessment

Note: This section (and activity) is required for HVAs (unless otherwise specified by the Authorizing Official or System Team) and is typically not performed for non-HVAs (unless otherwise specified by the Authorizing Official or System Team).

The Assessment Team will [scan and test wireless networks to ensure that appropriate safeguards are in place.] OR [review results of wireless scans and tests performed by <Wireless Assessor> on <Date> to ensure that appropriate safeguards are in place.]

### Configuration Review

Customize this section based on the scope of the assessment.

During the assessment, the Assessment Team will assess whether Security Capabilities are being implemented through reviewing switch, router, firewall, server, and software configurations, and network and application architecture diagrams to determine if the controls delineated by the applicable <Organization> policies, <Parent Organization> Minimum Security Configuration Standards for Departmental Operating Systems and Applications, and industry best practices (e.g., those outlined in the Router Security Configuration Guide published by the National Security Agency (NSA) and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG)) are being followed.

### Observances

During the assessment the Assessment Team will also scrutinize personnel and the physical environment, as applicable, to determine if security policies and procedures are being followed. Examples of areas that may be included are:

* If the Assessment Team staff are issued visitor badges
* If any form of identification is requested prior to visitor badge issuance
* How employees label and discard output materials
* Are monitors positioned to prevent “shoulder surfing” or viewing from windows and open spaces
* If telecommunication and wiring closets are locked

The Assessment Team will also conduct a datacenter tour to determine whether physical controls securing the information system and its data are adequate.

### Mainframe Batch Process Testing

Customize this section based on the scope of the assessment.

The Assessment Team will assess whether Security Capabilities are being implemented through evaluation of batch processes with the help of the appropriate System Administrator(s). The Assessment Team’s technical staff will work with the Mainframe Administrators to view essential, security-relevant settings and parameters of the batch files. Following is a list of activities the Assessment Team will perform:

* Verify and validate that batch processes can accomplish the specific tasks to meet business requirements
* Assess to determine if any Batch Automation Tools are used. If they are used, determine how batch processes are invoked by these tools and review command line parameters for appropriateness
* Review the nature of batch processes
* Assess the sequential nature of batch processes and the structure of different batch files
* Determine the regulatory constraints (i.e., auditing, traceability, etc.) with regards to batch processing and output results
* Examine to determine if sequence controls and batch process controls are implemented

### Mainframe System Testing

Customize this section based on the scope of the assessment.

The Assessment Team will assess whether Security Capabilities are being implemented through review of the mainframe implementation to ensure it is configured using the proper settings for protecting sensitive information, which will include the following:

* Inspect system security package configuration parameters
* Verify that proper configuration management procedures are being followed
* Examine access controls to system utilities, system datasets, and the system security program to determine appropriateness
* Determine if unnecessary services and protocols have been disabled
* Ensure that proper auditing is enabled
* Verify that the mainframe operating system and utility maintenance are being applied (e.g., Program Temporary Fixes [PTF] and Program Update Tapes [PUT]
* Examine user rights and privileges for files, jobs, and application regions
* Inspect vendor-installed exploits or “backdoors” (e.g., FTPs and databases)
* Examine backup and restore products and procedures

The Assessment Team will make a request to have several mainframe reports run before the team arrives onsite. These reports will help determine the mainframe’s security posture. The Assessment Team will provide the list of reports at least one week in advance of the assessment.

## Reporting

This section outlines how the Assessment Team will report vulnerabilities during the assessment.

### Findings Worksheet

The Findings Worksheet is a running tabulation of findings identified during the assessment that is provided to the system personnel as findings are identified.

### Reassignment of Findings

If, during the ACT testing period, a finding is determined to be outside the scope of the system or the responsibility of the System’s Business Owner and ISSO/ISSM, the finding will be assigned to the system being assessed and steps should be taken to reassign the finding to the correct system. The ISSO/ISSM should attempt to contact the correct system owner, provide them with the appropriate information, and invite them to be involved in the remaining ACT Security Assessment proceedings.

It is ultimately the responsibility of the System’s ISSO/ISSM to obtain agreement from the correct system owner to reassign the finding to it and follow through with the necessary reassignment steps prior to the Draft Security Assessment Report Review. If the correct system owner agrees to accept the finding, the ISSO/ISSM should inform the Assessment Team of the correct system’s official system name, acronym, and provide evidence of their acceptance of the finding; the Assessment Team will then report the finding as re-assigned in the Findings Worksheet and Security Assessment Report. If the ownership of the finding has not yet been successfully reassigned by the time of the Draft Report Review, the report will be finalized with the finding assigned to the currently-assessed system. It is then the responsibility of the ISSO/ISSM to address the reassignment after conclusion of the Security Assessment.

### Rating of SQL Injection and XSS Vulnerabilities

SQL Injection and Cross-Site Scripting (XSS) vulnerabilities have historically been frequently identified in assessments across <Organization> and MITRE’s other Federal government Sponsors. In accordance with rating and reporting norms across MITRE’s Sponsors, the Assessment Team will rate all SQL Injection and XSS vulnerabilities as HIGH-risk findings, regardless of whether the system is Internet-facing, unless otherwise directed by <Organization>.

### Test Reporting

The Assessment Team will conduct a Final Update meeting, if needed, after the assessment is completed. The Assessment Team might not have the opportunity to review all the provided documentation, configurations, and script outputs or data calls during the assessment phase; if this is the case, the Assessment Team will note this in the ACT Security Assessment Report.

Unless otherwise agreed by the ISSO/ISSM and the Assessment Team, the Assessment Team will provide the ACT Security Assessment Report and Findings Worksheet in Draft form within five business days following the last day of testing. System Team personnel will review the Draft Security Assessment Report and provide feedback within three business days following submission of the Draft, and the Assessment Team will update (as appropriate) and issue the Final ACT Security Assessment Report and Findings Worksheet within two business days following receipt of System Team feedback.

### Remediation Period

Due to the dynamic, rapid, and iterative pace of ACT assessments, unless otherwise agreed by the Assessment Team and system stakeholders, there is no Remediation Period during which the System Team can address findings for closure prior to reporting. All findings will be considered “final” once testing has concluded and will be recorded as “open” in the ACT Security Assessment Report.

1. POA&M: Plan of Action and Milestones [↑](#footnote-ref-2)