

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>)

Preliminary Intake Form

Table of Contents

[1. Points of Contact 1](#_Toc198584737)

[2. System Information 2](#_Toc198584738)

[2.1 Brief Description of System 2](#_Toc198584739)

[2.2 Access Mechanisms/Locations 3](#_Toc198584740)

[2.3 System Identification and Security Level 3](#_Toc198584741)

[2.4 Responsible Organizations 3](#_Toc198584742)

[2.5 System Type Designation and Categorization/Classification 3](#_Toc198584743)

[2.6 System Operational Status 5](#_Toc198584744)

[2.6.1 Authorization Boundary 5](#_Toc198584745)

[2.6.2 Assessment Boundary 6](#_Toc198584746)

[2.6.3 Prioritized Assessment 12](#_Toc198584747)

[3. System Artifacts 12](#_Toc198584748)

[3.1 Tier 1 – Minimum Security Artifacts 12](#_Toc198584749)

[3.2 Tier 2 – Supporting Artifacts 13](#_Toc198584750)

[3.3 Technical Output Artifacts 16](#_Toc198584751)

**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.

# Points of Contact

Please populate the following table with all applicable personnel information for each potential system role or responsibility. If a listed role is not applicable to your system, please leave the row in-place and mark the person’s Name as “N/A”. If any pertinent roles are missing, please add rows for them. If you have any questions, contact the ACT Team at [ACT@mitre.org](mailto:ACT@mitre.org).

Table . <System Acronym> Points of Contact

| Role | Name | Organization | Phone Number | Email Address |
| --- | --- | --- | --- | --- |
| Assessment POC: <Sponsor> |  |  |  |  |
| Assessment POC: <Contractor> |  |  |  |  |
| 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) |  |  |  |  |
| Information System Security Officer (ISSO) - 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 |  |  |  |  |

Specific points of contact must be identified for the following assessment preparation activities (if needed). Please populate the following table with all applicable contact information. If you have any questions, feel free to contact the ACT Team at [ACT@mitre.org](mailto:ACT@mitre.org).

Table . Assessment Preparation Activity Points of Contact

| Role | Name | Organization | Phone Number | Email Address |
| --- | --- | --- | --- | --- |
| Run scans/scripts for Assessment Team |  |  |  |  |
| Create test accounts for Assessment Team |  |  |  |  |
| Provide system overview/demo for Assessment Team |  |  |  |  |

# System Information

Please populate this section with all applicable system information. Some comments and examples (highlighted) are provided to assist. If you have any questions, feel free to contact the ACT Team at [ACT@mitre.org](mailto:ACT@mitre.org).

## Brief Description of System

Brief description of system:

TST is a special-purpose public website that provides training and customer support necessary to enable engineers to correctly fit hydrocoptic marzelvanes to a turbo-encabulator’s ambifacient lunar waneshaft in a manner that prevents side fumbling. TST completed its transition from the local data center to being hosted on Amazon Web Services (AWS) GovCloud in March 2024*.*

## 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/>

## System Identification and Security Level

Table 3. 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 4. Responsible Organizations

|  |  |
| --- | --- |
| Authorizing Official | * <Sponsor> Chief Information Security Officer (CISO) |
| System Owner / Responsible Organization | * <Sponsor> / 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 5. 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> |
| 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 6. System Operational Status

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

### Authorization Boundary

The following diagram clearly lays out the authorization boundary and can be found in the SSP:

A screenshot of a cell phone

Description automatically generated

Figure . Official Authorization Boundary Diagram

Provide any needed text description to clarify the diagram or provide information not clearly presented by the diagram.

#### Assessment Type and Scope

ACT Assessment Type(s) to be performed:

* ACT Security Assessment? **Yes**/No
* ACT Penetration Test? **Yes**/No
* ACT Risk Assessment? **Yes**/No

The following objects/components that fall within the system’s official authorization boundary are excluded from assessment during this assessment:

* Component 1
* Component 2
* Application 1
* Application 2
* *Etc.* …

### Assessment Boundary

The following tables detail System Information and the Assessment Boundary of this ACT [Security/Risk] Assessment / Penetration Test:

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 ISPG-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: <Sponsor> Primary Data Center (PDC) * <Address> * [Other] |
| Assessment Standards / Checks | * <Sponsor-specified Security Controls Catalog> * FedRAMP High / Moderate / Low * Industry Best Practices * [Others…] |

Table . ACT Penetration Test Scope Specification

|  |  |
| --- | --- |
| Assessment Type | * ACT Pen Test (Application + Infrastructure) * ACT Pen Test (Application-Only) * ACT Pen Test (Infrastructure-Only) |
| Core Controls / Capabilities Included? (If not, explain why not) | * Yes / No |
| 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) | * Testing: <Sponsor> Primary Data Center (PDC) * <Address> * [Other] |
| Assessment Standards / Checks | * <Sponsor-specified Security Controls Catalog> * FedRAMP High / Moderate / Low * Industry Best Practices * [Others…] |

Table . ACT Risk Assessment Scope Specification

|  |  |
| --- | --- |
| Risk Information Sources | * A123 Audit * ACT Risk Assessment * ACT Security Assessment * CDM Data Sources * Information System Risk Assessment (ISRA) * Penetration Testing * POA&Ms – System * POA&Ms – Inherited * Privacy Impact Analysis (PIA) * Risk Vulnerability Assessment (RVA) * Security Controls Assessment (SCA) * Security Impact Analysis (SIA) * Self-Assessment * Technical Review Board (TRB) * Vulnerability Scans * [other] |
| Assessment Dates | * May 12-16, 2025 |
| Assessment Location(s) | * Risk Analysis: Remote via [mechanism] * [Other] |

### Prioritized Assessment

<List and describe any components, features, functions, security controls, etc. that you would like for the Assessment Team to emphasize or focus on during the assessment:

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

# System Artifacts

## Tier 1 – Minimum Security Artifacts

These artifacts should be provided for use in the development of the Assessment Plan, *or an explanation about why they are not available (or not applicable) must be provided*. These artifacts are extremely helpful in determining the system authorization boundary, devices in scope, number of components, system complexity, etc. Each should be updated and provided to the Assessment Team prior to the upcoming Preliminary Discussion. Please prepend each filename with the appropriate label from the “Artifact ID” column:

Table . Tier 1 Artifacts – Minimum Security Documentation

| **Artifact ID** | **Document/Information Requested** |
| --- | --- |
| 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 – Supporting Artifacts

In addition to the Tier 1 Artifacts, the following artifacts (labeled “Tier 2 Artifacts”) should also be updated and provided to the Assessment Team prior to the upcoming Preliminary Discussion, *or an explanation about why they are not available (or not applicable) must be provided*. Please prepend each filename with the appropriate label from the “Artifact ID” column:

Table . Tier 2 Artifacts – Supporting Artifacts

| **Artifact ID** | **Document/Information Requested** |
| --- | --- |
| 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 * 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

The Assessment Team will also 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 CMS 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** |
| --- | --- |
| 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.* |

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