

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 Report (SAR)

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. Executive Summary 1](#_Toc198646001)

[2. Security Assessment Summary 3](#_Toc198646002)

[2.1 Summary of Identified Compliance Findings 1](#_Toc198646003)

[2.1.1 System Findings 1](#_Toc198646004)

[2.1.2 Findings Recommended for Reassignment 2](#_Toc198646005)

[2.2 System Observations 3](#_Toc198646006)

[2.3 Plan of Action and Milestones (POA&M) Validation Status 3](#_Toc198646007)

[2.4 Summary of Recommendations 1](#_Toc198646008)

[3. System Information 2](#_Toc198646009)

[3.1 Brief Description of System 2](#_Toc198646010)

[3.2 System Identification and Security Level 2](#_Toc198646011)

[3.3 Responsible Organizations 2](#_Toc198646012)

[3.4 System Type Designation and Categorization/Classification 2](#_Toc198646013)

[3.5 System Operational Status 3](#_Toc198646014)

[4. Security Assessment Scope and Methodology 4](#_Toc198646015)

[4.1 Security Assessment Scope 4](#_Toc198646016)

[4.1.1 Authorization Boundary Description 4](#_Toc198646017)

[4.1.2 Assessment Boundary Description 6](#_Toc198646018)

[4.1.3 Prioritized Assessment 13](#_Toc198646019)

[4.1.4 Core Controls 13](#_Toc198646020)

[4.1.5 Untested Portions of In-Scope System 14](#_Toc198646021)

[4.2 Security Assessment Methodology 14](#_Toc198646022)

[4.2.1 Level of Testing Rigor 15](#_Toc198646023)

[4.2.2 Vulnerability Assessment 16](#_Toc198646024)

[4.2.3 Tests and Analyses 17](#_Toc198646025)

[4.2.4 System Configuration Review 19](#_Toc198646026)

[4.2.5 Documentation Review and Interviews 19](#_Toc198646027)

[Appendix A. Risk Scoring Methodology 21](#_Toc198646028)

[A.1. Risk Level Assessment 21](#_Toc198646029)

[A.2. Impact Severity 21](#_Toc198646030)

[A.3. Likelihood of Occurrence 22](#_Toc198646031)

# 

# Executive Summary

“Does this system pose an abnormal risk?”

Provide the BLUF (Bottom-Line Up-Front): The AO should be able to read only the Executive Summary and know whether she wants to grant ATO now or read further into the report for further details. Using plain language, synopsize in approximately three brief paragraphs the following points:

**Scope of Assessment:**

* Which system components (etc.) were in and out of scope?
* Which Capabilities (etc.) were in and out of scope?
* Which assessment activities were conducted (i.e., was this an atypical assessment)?

**What Was Found:**

* What categories of Findings / Corrective Actions were identified?

**What Do The Findings Mean:**

* What do the Findings indicate about the past, present, and future security posture of the system?
* How do the Findings impact System and Enterprise?
* (If applicable) How do the Findings compare to those of other similar systems?

Note: Each bullet point above should be as detailed as necessary to tell the appropriate story for this particular ACT. For example, if Technical Testing was not performed for some reason, that should be specifically called out; but if all normal assessment activities were performed then little needs to be said.

Example text is below – edit or replace with appropriate new text:

The <Organization> engaged <Assessment Contractor> (the “Assessment Team”) to conduct a [comprehensive-scope / tailored-scope] [application-only / infrastructure-only / application + infrastructure] Adaptive Capabilities Testing (ACT) Security Assessment of <System Name> (<System Acronym>) as part of the <Organization> Assessment and Authorization (A&A) Program. <System Acronym> is owned by <division / group> and <operated/developed/maintained> by <Contractor>.

[Provide a very brief description (~one paragraph) of the assessed system].

The Security Assessment was conducted from <list dates>, [included the entire authorization boundary / excluded the [specify portion(s)] because [reason(s)]], and focused on [a specific subset of / all] Security Capabilities. [Interviews, document reviews, evidence examinations, and technical testing] were conducted which identified areas of non-compliance (called “findings”).

For each finding the Assessment Team developed detailed recommendations for improvements that address the finding and strengthen overall <Organization> information security. Highlights of the finding recommendations are summarized below, with references to specific findings in parentheses:

* **EXAMPLE: Strengthen User Authentication:** Reduce likelihood of beneficiary impersonation by strengthening authentication requirements for Internet users (F01). Implement Multifactor Authentication (MFA) for administrators (F03).
* **EXAMPLE: Update Documentation:** Update the SSP to document the correct accreditation boundary, control implementations, and control inheritance (F06). Update and test the Contingency Plan (F05).
* **EXAMPLE: Implement Denial of Service (DoS) Protections:** Work with providing Data Center to enable connection throttling and other DoS mitigations (F02).
* **EXAMPLE:** Address Technical Architecture Noncompliance: Move the Admin Workstation to a newly-implemented compliant Management Band (F04).

[If applicable, describe any particularly noteworthy anomalies (positive or negative) here.] These weaknesses are [typical / atypical] of similar systems deployed within the <Organization> Enterprise. See the separate Risk Assessment Report for analysis of the risks posed by these findings.

# Security Assessment Summary

This section (and its subsections) should clearly and quickly answer these questions:

**“How did the Security Assessment go?”**

**“What is the current state of the system?”**

**“What should we do as a result of this ACT?”**

The purpose of this ACT Security Assessment Report is to clearly explain the information the Assessment Team obtained prior to the assessment, the areas that were examined during the assessment, and the detailed results of 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”).

The ACT process facilitates a holistic view of <sponsor’s> organizational and system risk posture by focusing assessment on mature execution of Security Capabilities derived from NISTIR[[1]](#footnote-2) 8011. This ACT Security Assessment focused on assessing <System Acronym>’s current implementation of the Security Capabilities and Sub-Capabilities by determining the system’s compliance with the various Acceptable Risk Safeguards (ARS) security controls that map to those Security Capabilities (including the *<Organization> Core Controls*), and by performing other testing and analysis as-appropriate. The result of this Security Assessment is the set of Findings listed in Section 2.1.

The System Team provided the Assessment Team with excellent support during the engagement. Before the start of the assessment phase, the System Team provided the Assessment Team with [all / some of the] documentation and other artifacts requested in the ACT Assessment Plan. During the assessment phase, [all / some] required personnel were [not] available for interviews, questions were answered promptly, additional artifact requests were fulfilled, and the system was [not] available and ready for technical testing.

[If any of the Core Controls were not fully or adequately tested, succinctly state this and explain the reason(s) why. For example: “<Organization> directed the Assessment Team not to assess Core Control CM-02 because, at the time of this ACT, the system was still being developed and implemented, and the baseline configuration had not yet been defined.”]

## Summary of Identified Compliance Findings

“What were the low-level test results?”

This section describes the deviations from requirements that were identified through the ACT Security Assessment process. Each finding is thoroughly explained and corrective actions for closing or reducing the impact of each vulnerability are recommended. More details for each finding are in the separate findings data file.

Table . Explanation of Findings

| Sub-Capability | Security Control(s) | Finding ID | Finding Description | Weakness Description | Test Result Description | Recommended Corrective Action(s) | Status, Risk, Impact, Likelihood |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Affected Sub-Capability (e.g., “BEHAVE-02”) | Affected <Organization> Security Control (e.g., “AU-05”) | Unique ID for this finding, generated by Assessment Team. | Describes a deficiency, related to one or more Controls or Sub-Capabilities. | The effect of the deficiency within the system, and how it affects the Sub-Capability and Capability for the system and for the larger <Organization> enterprise. | The actual results from the test/assessment (i.e., the actual state vs. the intended state). | Recommended steps for remediating the weakness. | Status: [Open/Closed]  Risk Level: [Calculate: see Appendix]  Impact: <See Appendix>  Likelihood: <See Appendix> |

### System Findings

The following Findings were identified during this ACT Security Assessment and apply to the assessed system:

Table . Findings

| Sub-Capability | Security Control(s) | Finding ID | Finding Description | Weakness Description | Test Result Description | Recommended Corrective Action(s) | Risk, Impact, Likelihood |
| --- | --- | --- | --- | --- | --- | --- | --- |
| <Sub-Capability ID> | <Control ID> | <Finding ID> | <Finding Description> | <Weakness Description> | <Test Result Description> | <Recommended Corrective Action(s)> | Status: [Open/Closed]  Risk Level: [Calculate: see Appendix]  Impact: <See Appendix>  Likelihood: <See Appendix> |

### Findings Recommended for Reassignment

The following Findings were identified during this ACT Security Assessment, but the system ISSO recommends that they be reassigned to other systems. It is the responsibility of the system ISSO to coordinate reassignment with the ISSO of the receiving system. If the Finding is not formally accepted by the other system, then the finding remains the responsibility of this system.

Table . Findings Recommended for Reassignment

| Reassign To: | Sub-Capability | Security Control(s) | Finding ID | Finding Description | Weakness Description | Test Result Description | Recommended Corrective Action(s) | Status, Risk, Impact, Likelihood |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| <Information System or Program Name> | <Sub-Capability ID> | <Control ID> | <Finding ID> | <Finding Description> | <Weakness Description> | <Test Result> | <Recommended Corrective Action(s)> | Status: [Open/Closed]  Risk Level: [Calculate: see Appendix B]  Impact: <See Appendix>  Likelihood: <See Appendix> |

## System Observations

The following Observations were identified during this ACT Security Assessment and apply to the assessed system. Observations allow the Assessment Team to highlight specific areas of concern without generating a formal finding of non-compliance.

Table . Observations

| Sub-Capability | Security Control(s) | Observation ID | Observation Description |
| --- | --- | --- | --- |
| <Sub-Capability ID> | <Control ID> | <Observation ID> | <Observation Description> |

## Plan of Action and Milestones (POA&M) Validation Status

The Assessment Team was not tasked with validating any POA&Ms.

The Assessment Team was tasked with validating POA&Ms with a status of Pending Verification or Completed. At the time of this ACT Security Assessment the system had <number of open POA&Ms> open POA&Ms, of which <number of POA&Ms reviewed> were reviewed to determine whether sufficient evidence existed to close them. The remaining <number of POA&Ms not reviewed> POA&Ms were not reviewed because <reason POA&Ms were not reviewed>. This section contains the status of POA&Ms that have been validated, as well as POA&Ms for which adequate evidence was not provided to warrant closure.

The following table details the POA&Ms that remain open after the Assessment Team’s review:

Table 5. Reviewed POA&Ms That Remain Open

| <GRC tool> Weakness ID | Risk Level | Weakness (copied from <GRC tool>) | Re-Assessment Comment |
| --- | --- | --- | --- |
|  |  |  |  |

The following table details the POA&Ms that have been verified by the Assessment Team as being successfully remediated, and are recommended for closure:

Table 6. Reviewed POA&Ms Recommended for Closure

| <GRC tool> Weakness ID | Risk Level | Weakness (copied from <GRC tool>) | Re-Assessment Comment |
| --- | --- | --- | --- |
|  |  |  |  |

## Summary of Recommendations

“What should we do?”

Based on the findings identified above, the assessment team recommends that the system team consider taking the following actions:

* **Update Software to Latest Patch Levels:** Expedite the testing of all available software and operating system patches – especially those with security content – in the test environment and then deploy them to Production. Ensure that the documented configuration management process is followed.
* **Address Insecure Cryptographic Functions:** Several cryptographic modules within the assessment boundary allowed the use of non-approved algorithms, indicating that the modules are either misconfigured or do not support the approved cryptographic algorithms. Update the code and/or configuration of these modules to implement approved algorithms and to meet all other documented configuration and operational requirements.

# System Information

## Brief Description of System

<Brief description of the system.>

## System Identification and Security Level

Table 7. 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 8. 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 9. 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 10. System Operational Status

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

# Security Assessment Scope and Methodology

**“What was assessed?”**

**“How was it assessed?”**

## Security Assessment Scope

**“What was and wasn’t assessed?”**

The reader should be able to clearly understand what was 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 actual scope.

### Authorization Boundary Description

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

Copy/paste the system’s official accreditation boundary diagram from the SSP.

If the diagram, when pasted into this template, does not clearly and unambiguously identify the accreditation boundary, 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.

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.

A screenshot of a cell phone

Description automatically generated

Figure 1. <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 the System Team 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 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 2. <System Acronym> Updated Authorization Boundary Diagram

### Assessment Boundary Description

Based on this definition of the authorization boundary, <Organization> division / group> directed the Assessment Team to assess [the entire system / certain portions of the system], as shown in Figure 3 by the red dashed boxes in the following assessment boundary diagram copied from the final Security Assessment Plan:

A screenshot of a cell phone

Description automatically generated

Figure 3. <System Acronym> Assessment Boundary from Security Assessment Plan

During the assessment phase, the assessment boundary was modified by the System Team because <reason(s) for assessment boundary modification>. The final, modified assessment boundary is identified by the red dashed boxes in Figure 4:

A screenshot of a map

Description automatically generated

Figure 4. <System Acronym> Final Assessment Boundary

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 from the system’s [official / updated] authorization boundary diagram were 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 were:

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 |

### Untested Portions of In-Scope System

**“What did we intend, but were unable, to assess?”**

Explain why anything in-scope was NOT assessed. The prioritization issues in the previous subsections are one of many reasons why in-scope objects might not have been tested. If everything in-scope was tested, say so. Be sure that this section aligns with the scope diagram(s) and scope table.

[All portions of the in-scope system were tested.]

[The following items were in-scope but not assessed during this ACT Security Assessment:

* EXAMPLE: The Cisco 5620 switch was not tested because the system team took it down for maintenance on Friday (April 30) before the assessment began, and it was not restored to operation by the end of the assessment phase. The development team declined to provide configuration data for the switch.
* [Capability/control/component/function/system/etc.] was not assessed because [reason].]

## Security Assessment Methodology

**“What assessment steps were and weren’t taken?”**

Since the reader likely comes with many assumptions based on their understanding of the standard activities included in a typical Security Assessment, the SAR must explicitly correct those assumptions when they are not met. <Organization> expects and requires every ACT Security Assessment to (by default) include the activities listed in the template text below – if any of these activities were NOT included, or were not conducted at the level of detail and rigor that <Organization> typically expects, then this must be explicitly explained here (and in other appropriate locations throughout the document).

The Assessment Team comprised the following personnel:

Table . Assessment Team Members

| Name | Role | Phone Number | Email Address |
| --- | --- | --- | --- |
| <First Last> | Assessment Lead | <xxx-xxx-xxxx> | <Email Address> |
| <First Last> | M&O Assessor | <xxx-xxx-xxxx> | <Email Address> |
| <First Last> | Application Assessor | <xxx-xxx-xxxx> | <Email Address> |
| <First Last> | Application Assessor | <xxx-xxx-xxxx> | <Email Address> |
| <First Last> | DB Assessor | <xxx-xxx-xxxx> | <Email Address> |
| <First Last> | OS Assessor | <xxx-xxx-xxxx> | <Email Address> |
| <First Last> | Network Assessor | <xxx-xxx-xxxx> | <Email Address> |
| <First Last> | Mainframe Assessor | <xxx-xxx-xxxx> | <Email Address> |
| <First Last> | Privacy Assessor | <xxx-xxx-xxxx> | <Email Address> |
| Cloud Assessor | <First Last> | <xxx-xxx-xxxx> | <Email Address> |
| Virtualization Assessor | <First Last> | <xxx-xxx-xxxx> | <Email Address> |

The Assessment Team assessed <System Acronym> and its environment by conducting interviews of key personnel, technical testing and technical vulnerability assessment, system configuration assessment, policy compliance assessment, and documentation review. [Describe any caveats, such as the omission of expected activities such as thorough technical testing, interviews, etc.]

This approach provided the team with an accurate and comprehensive understanding of the current deployment of <System Acronym>. The main objectives of the ACT Security Assessment were to determine:

* If the system adequately implemented the <Organization> Core Controls.
* If the system adequately implemented the <Organization> Security Capabilities, and that it was in compliance with the latest published versions of the *<Organization> <List all applicable guidance and policies>.*
* If the system’s infrastructure components were securely implemented.
* If the inherited infrastructure components were security implemented.
* If the application was securely maintained.
* If the database was configured properly.
* Vulnerabilities and their potential impact.
* Weak system configuration settings that, if not changed, could compromise the CIA[[2]](#footnote-3) of system data.
* Where established <Organization> security policies have not been followed.
* Major discrepancies in system documentation.
* Weaknesses in the Configuration Management (CM) process.
* Weaknesses in program management.

### Level of Testing Rigor

Since the goal of a Security Assessment is to determine both the system’s actual compliance with Security Controls and the correctness and reliability of the system’s 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 the <SPONSOR Security Control policy>. These Levels are described in the table below:

Table . Levels of Testing Rigor



The Assessment Team tailored their assessment methods to meet the verification objectives of Testing Rigor Level <Testing Rigor Level>, which was chosen by <Organization> for this Security Assessment.

### Vulnerability Assessment

The type of technical testing performed during the ACT Security Assessment comprised 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.

The Vulnerability Assessment evaluated the system’s vulnerability to insider attacks, network-based attacks, and weaknesses in the management and operational areas of the <<Organization> division / group> and <Contractor> security programs. To accomplish this objective, the Assessment Team developed an accurate and comprehensive understanding of how the system was configured to determine what an adversary could learn about, and subsequently exploit, in the operational environment. However, the Vulnerability Assessment stopped once the determination was made that a vulnerability could (or could likely) be exploited – the Assessors did not attempt to fully exploit and escalate the vulnerabilities (as a Penetration Test would).

The ACT Security Assessment was conducted with full knowledge of the system, products, configurations, and topology. To determine the system configuration and complete a vulnerability assessment of the application, the ACT Security Assessment looked for the following:

* Improper, weak, or vulnerable configurations
* Non-standard configurations
* Published or known weaknesses, bugs, advisories, and security alerts about specific hardware, software, and networking products used in the system
* Failure to comply with <Organization> security policies and procedures

### Tests and Analyses

The ACT Security Assessment included several tests that methodically analyzed the <System Acronym> application and infrastructure. These tests began with high-level scans, and then increased in their specificity to include an analysis of each component. The types of tests and analyses the team performed during this assessment included the following:

* **Application Assessment** **–** subjected the applications to manual and automated testing to ensure the protection of data processed by the application
* **Automated Scanning –** subjected the infrastructure to the same type of scripted scanning attacks that are available via commercial products and public domain tools
* **Best Engineering Judgment and Various Ad Hoc Tests –** verified that specific requirements, previous recommendations, and conditions had been satisfied
* **Database Scanning –** subjected the underlying database to automated scripts to discover any vulnerabilities in the database configuration
* **Network Mapping and Asset Discovery –** utilized automated tools to scan specific network segments to discover active systems, and the services offered by those systems
* **Penetration Testing** – [attempted to gain access to the system via typical penetration testing techniques with [full / limited] knowledge of the system] OR [reviewed results of penetration testing performed by <Penetration Test Assessor> on <Date>]
* **Personnel Interviews –** interviewed various personnel involved with the daily operational maintenance of the system, as well as other personnel tasked with protecting the system
* **Shoulder Surfing –** assessed the system through observation of the System Administrators performing testing actions on behalf of the Assessment Team
* **System Configuration Review –** ran automated scripts and used direct observation to analyze the configuration of network components
* **Wireless Assessment –** [scanned and tested wireless networks to ensure that appropriate safeguards are in place.] OR [reviewed results of wireless scans and tests performed by <Wireless Assessor> on <Date> to ensure that appropriate safeguards are in place.]

#### Tools Used

The Assessment Team worked with the System Team to ensure that industry best practices are reflected in the system’s architecture and design. The tools used by the team during the assessment are listed below:

Table . Tools Used

| 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 <Organization>’s assessment contractors 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. |
| [GoBuster](https://github.com/OJ/gobuster) | Used to brute-force: URIs (directories and files) in web sites; DNS subdomains (with wildcard support); and Virtual Host names on target web servers. |
| [InSpec](http://inspec.io/) | Open-source testing framework for infrastructure with a human- and machine-readable language for specifying compliance, security and policy requirements. |
| [Maltego](https://www.paterva.com/) | 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](https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon) | Open source, offensive security framework comprised of [PowerShell](https://attack.mitre.org/techniques/T1086) modules and scripts that perform a wide range of tasks related to penetration testing such as code execution, persistence, bypassing anti-virus, recon, and exfiltration. |
| SCAP Compliance Checker (SCC) & CIS CAT PRO | Allow the comparison of systems against various baseline standards. These include CIS level 1, level 2, and DISA STIGs.  *Note: Require memberships to MAX.gov and CIS for download.* |
| [Sn1per](https://github.com/1N3/Sn1per) | 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/) | 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) | 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 proxy. |

### System Configuration Review

The main objectives of the system configuration review were to determine if <Organization> division / group>’s Security Capabilities and underlying <SPONSOR Security Control Policy> requirements were properly implemented. For this review, the Assessment Team took the following actions:

* Conducted host-based assessments to determine current configurations for each system
* Tested firewalls, routers, applications, and databases for default user accounts
* Reviewed firewall access control rules
* Reviewed switch configurations
* Determined if system configurations aligned with system documentation

### Documentation Review and Interviews

The main objectives of the documentation review and interviews were to determine if the system personnel accurately and adequately understand and document the functions and security posture of the assessed system. For this review, the Assessment Team took the following actions:

* Reviewed and provided feedback on the System Security Plan (SSP)
* Reviewed and provided feedback on the Information System Risk Assessment (ISRA)
* Reviewed and provided feedback on the Contingency Plan (CP)
* Reviewed and provided feedback on the Privacy Impact Analysis (PIA)
* Reviewed other Tier 1, Tier 2, and Tier 3 artifacts:
  + [List other artifacts reviewed during assessment phase.]
* Conducted interviews of:
  + Application Developer: <App Dev name>
  + Business Owner: <BO name>
  + Configuration Manager: <Config Manager name>
  + Contingency Manager: <Contingency Manager name>
  + Cyber Risk Advisor (CRA): <CRA name>
  + Database Administrator: <DB Admin name>
  + Database Administrator (DB2 Central DBA): <DB2 Central DBA name>
  + Database Administrator (DB2 System Programmer): <DB2 Sys Programmer name>
  + Datacenter/Facilities Manager: <Facilities Manager name>
  + Firewall Administrator: <FW Admin name>
  + Human Resources Manager: <HR Manager name>
  + Incident Handling Manager: <Incident Manager name>
  + Information System Security Manager (ISSM): <ISSM name>
  + Information System Security Officer (ISSO): <ISSO name>
  + Mainframe Administrator: <Mainframe Admin name>
  + Media Custodian: <Media Custodian name>
  + Middleware Utilities Administrator: <Middleware Admin name>
  + Network Administrator: <Network Admin name>
  + Privacy Subject Matter Expert (PSME): <PSME name>
  + Program Manager: <PM name>
  + Security Utilities Administrator: <Security Utils Admin name>
  + System Administrator: <SysAdmin name>
  + System Owner: <System Owner name>
  + Training Manager: <Training Manager name>

1. Risk Scoring Methodology

A Risk Level value must be assigned to each finding in order to provide a guideline by which to understand the procedural or technical significance of each finding.

* 1. Risk Level Assessment

Each finding will be assigned a Risk Level value of “Critical”, “High”, “Moderate”, or “Low” as defined in Table 17 below. This rating is, in effect, an assessment of the priority for addressing each finding.

Table . Risk Level Definitions

| Rating | Definition of Risk Rating |
| --- | --- |
| Low | Exploitation of the technical or procedural vulnerability will cause minimal impact to the Organization’s operations. The confidentiality, integrity and availability of sensitive information are not at risk of compromise. Exploitation of the vulnerability may cause slight financial loss or public embarrassment. |
| Moderate | Exploitation of the technical or procedural vulnerability will significantly impact the confidentiality, integrity and/or availability of the system or data. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment to the Organization. |
| High | Exploitation of the technical or procedural vulnerability will cause substantial harm to the Organization’s business processes. Significant political, financial, and legal damage is likely to result. |
| Critical | Exploitation of the technical or procedural vulnerability will cause catastrophic adverse effects to the Organization’s operations, organizational assets, individuals, other organizations, or the Nation. Significant political, financial, and legal damage is very likely to result. |

The Risk Level is calculated in Table 18:

Table . Risk Level Determination

| Likelihood of Occurrence | Impact Severity | | | | |
| --- | --- | --- | --- | --- | --- |
| Low | Moderate | High | Critical |
| **Low** | Low | Low | Low | Moderate |
| **Moderate** | Low | Moderate | Moderate | High |
| **High** | Low | Moderate | High | Critical |
| **Critical** | Low | Moderate | High | Critical |

* 1. Impact Severity

For each finding, a determination will be made of the magnitude or severity of impact on (1) the business function if the existing controls and business rules are applied and the threat still materializes, and (2) the system’s operational capabilities and data if the threat is realized and exploits the associated vulnerability.

Table . Impact Definitions

| Rating | Definition of Impact Rating |
| --- | --- |
| Low | Will have some minor effect on the business function/system.  Might cause minor financial loss, but will not result in negative publicity or political damage.  Will require only minimal effort to complete corrective actions and continue or resume operations.  Will require minimal effort to repair or reconfigure the system. |
| Moderate | Will result in some tangible harm, albeit negligible, and perhaps only realized by a few individuals or agencies.  Might cause political embarrassment, negative publicity, and moderate financial loss.  Will require a moderate expenditure of resources to repair. |
| High | Might cause damage to the reputation of system management, the Organization, and/or notable loss of confidence in the ability for the Organization to complete its stated business mission, system resources and services.  Might result in legal liability and will require significant expenditure of resources to repair or to complete corrective actions and restore operations.  Might cause system outage or other considerable disruption in the business function  Might require recovery in an alternate site environment or hot-site environment.  Might result in compromise of large amount of Government information or services, a substantial financial loss, and the failure to deliver the Organization’s public programs and services. |
| Critical | Might be expected to have multiple severe or catastrophic adverse effects on the Organization’s operations, organizational assets, individuals, other organizations, or the Nation.  Might cause damage to the reputation of system management, the Organization, and/or notable loss of confidence in the ability for the Organization to complete its stated business mission, system resources and services.  Might result in legal liability and will require significant expenditure of resources to repair or to complete corrective actions and restore operations.  Might cause system outage or other considerable disruption in the business function.  Might require recovery in an alternate site environment or hot-site environment.  Might result in compromise of large amount of Government information or services, a substantial financial loss, and the failure to deliver the Organization’s public programs and services. |

* 1. Likelihood of Occurrence

For each finding, a determination will be made of the likelihood that a threat will materialize or that a threat will exploit any vulnerability. The likelihood is an estimate of the frequency or the probability of a threat materializing or that a threat will exploit any vulnerability.

Table . Likelihood Definitions

| Rating | Definition of Likelihood Rating |
| --- | --- |
| Low | Likely to occur once every year or less. |
| Moderate | Likely to occur once every six months or less. |
| High | Likely to occur once per month or more. |
| Critical | Likely to occur once per week or more. |

1. NISTIR: National Institute of Standards and Technology (NIST) Interagency Report (IR) [↑](#footnote-ref-2)
2. CIA: Confidentiality, Integrity, Availability [↑](#footnote-ref-3)