

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>)

Risk Assessment Report (RAR)

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](#_Toc198646377)

[2. Risk Assessment Summary 3](#_Toc198646378)

[2.1 Summary of Identified Compliance Findings 4](#_Toc198646379)

[2.1.1 Inherent Risks 4](#_Toc198646380)

[2.1.2 Residual Risks 8](#_Toc198646381)

[2.1.3 Inherited Risks 10](#_Toc198646382)

[2.2 Summary of Recommendations 11](#_Toc198646383)

[3. System Information 12](#_Toc198646384)

[3.1 Brief Description of System 12](#_Toc198646385)

[3.2 System Identification and Security Level 12](#_Toc198646386)

[3.3 Responsible Organizations 12](#_Toc198646387)

[3.4 System Type Designation and Categorization/Classification 12](#_Toc198646388)

[3.5 System Operational Status 13](#_Toc198646389)

[4. Risk Assessment Scope and Methodology 14](#_Toc198646390)

[4.1 Risk Assessment Scope 14](#_Toc198646391)

[4.1.1 Authorization Boundary Description 14](#_Toc198646392)

[4.1.2 Assessment Boundary Description 16](#_Toc198646393)

[4.2 Risk Assessment Methodology 19](#_Toc198646394)

[5. Risk Information Sources 20](#_Toc198646395)

[Appendix A. Risk Scoring Methodology 1](#_Toc198646396)

[A.1. Risk Level Assessment 1](#_Toc198646397)

[A.2. Impact Severity 1](#_Toc198646398)

[A.3. Likelihood of Occurrence 2](#_Toc198646399)

# 

# 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 Risk Assessment:

* Which Risk Information Sources were available or unavailable?
* Which system components (etc.) were in and out of scope?
* Which Capabilities (etc.) were in and out of scope?
* Which risk assessment activities were conducted (i.e., was this an atypical risk assessment)?

What Was Found:

* What categories of Risks were identified?

What Do the Risks Mean:

* How do the Risks impact System and <Organization> Enterprise?
* (If applicable) How do the Risks compare to 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 [a / an] Adaptive Capabilities Testing (ACT) Risk 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].

This Risk Assessment was performed at the same time as an ACT Security Assessment, and inherits the following limitations and assumptions from that Security Assessment:

* <Pertinent (not all) limitations and/or assumptions inherited from the Security Assessment that help explain or contextualize the Risks – if it’s not important, don’t list it here in the Executive Summary>

The Risk Assessment focused on [a specific subset of / all] Security Capabilities, [included the entire authorization boundary / excluded the [specify portion(s)] because [reason(s)], and utilized a [typical / smaller than normal / larger than normal / [other]] set of Risk Information Sources (RIS). Analysis of these RIS identified risks that might result in:

* Lateral movement by malicious users from this to other <Organization> systems
* Insecure or inadequate configuration or functionality
* Data leakage, alteration, or destruction on this and other <Organization> systems
* System unavailability
* Congressional inquiry
* Reputational damage
* Financial loss

[If applicable, describe any particularly noteworthy anomalies (positive or negative) here.] [These / Most of these] risks are [typical / atypical] of similar systems deployed within the <Organization> Enterprise and indicate that the system poses a [normal / lower-than-normal / higher-than-normal] overall level of risk to the <Organization> Enterprise.

# Risk Assessment Summary

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

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

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

The purpose of this ACT Risk 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 <Organization>’s organizational and system risk posture by focusing assessment on mature execution of Security Capabilities derived from NISTIR1 8011. This ACT Risk Assessment focused on assessing the risks posed by <System Acronym>’s current implementation of <Organization>’s Security Capabilities by evaluating the various available Risk Information Sources listed in Section 5. The result of this Risk Assessment is the set of Risks listed in Section 2.1.

## Summary of Identified Compliance Findings

“What risks arose from the the low-level test results?”

### Inherent Risks

“What are the concerns from this risk assessment that arise from open/unmitigated findings or other issues?”

*Inherent* risks are those that arise directly from unmitigated findings (including open Plan of Action and Milestones (POA&Ms)).

[The following table **summarizes** the identified inherent risks related to each assessed Security Capability; details about these can be found in the various Risk Information Sources and related artifacts listed for each risk.] OR [This Risk Assessment did not identify any inherent risks.]

The following table provides an example Risk for the author’s reference, and must be deleted before submission. This example Risk is drawn from the TST Sample RAR that is included as an attachment to the ACT Assessment Handbook.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Risk ID | *TST-20191104-R01* | | Impact | | *Low* | | Likelihood | *Critical* | | Risk Level | *Low* |
| Risk Title | *Weak authentication on Admin Workstation* | | | | | | | | | | |
| Capability | *CRED: Manage Credentials and Authentication* | | | | Sub-Capability ID | | *CRED-01* | Sub-Capability Name | | *Prevent users from unauthorized access* | |
| Capability | *DBS: Design and Build-in Security* | | | | Sub-Capability ID | | *DBS-01* | Sub-Capability Name | | *Define DBS Security CONOPS* | |
| Potential Cause | *Inadequate access controls on management interface* | | | | | | | | | | |
| *(“…causing…”)* Potential Event | *Unrestricted sabotage or reconnaissance of system* | | | | | | | | | | |
| *(“…resulting in…”)* Potential Consequence | *Unavailability of system; compromise of other <Organization> systems; Incorrect data used across <Organization> systems; damage to <Organization> reputation; financial compensation to beneficiaries; Congressional inquiry* | | | | | | | | | | |
| RIS | *Penetration Test* | RIS Artifact | | SOC Penetration Test Results | | RIS Artifact Element(s) | | | *SOC-20241002-F17* | | |
| RIS | *ACT Security Assessment* | RIS Artifact | | TST ACT Report – Security Assessment | | RIS Artifact Element(s) | | | *TST-20241104-F03, TST-20241104-F06* | | |
| Narrative | *The “Admin Workstation” in the Data Zone requires only a single authentication factor (a password), which makes this critical system component more susceptible than other components to credential guessing and/or compromise. The following risk information helps to either mitigate or exacerbate this weakness:*   * *The Firewall rules ensure that no traffic to or from the Admin Workstation is allowed to traverse the DMZ – traffic is only allowed to/from the Contractor VPN (since it is connected to the Switch on the Data Zone side of the Firewall).* * *While the Database Server, which is connected to the same Switch, is itself directly connected to the PrivateNET for LDAP access, firewall rules at the PrivateNET demarcation point allow only traffic to and from LDAP.* * *The SOC Penetration Test included descriptions of the robust and thorough physical and logical security controls, policies, and procedures in place at the Contractor facilities (connected via the Contractor VPN). The Contractor Workstation(s) connected via the Contractor VPN are hosted on a physically isolated network (not connected to the Internet nor to any other Contractor network), only contractors with administrative privileges are allowed to access the network, and the facility operates under Security Operations Center (SOC)-like procedures and controls.* * *Incorrect documentation and lack of proactive awareness and action by system personnel caused the Firewalls to be unmanaged by anyone for a period of at least three (3) years before this was identified by the ACT Security Assessment Team.*   *As long as the Firewalls and other security architecture are maintained as currently intended, and as long as the Contractor VPN endpoint network is secured as it currently is, the risk of exploitation of this weakness is Low.* | | | | | | | | | | |

Table . Inherent Risk <Risk ID>: <Risk Title>

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Risk ID** | <Risk ID> | | **Impact** | | <Risk Impact> | | **Likelihood** | | <Risk Likelihood> | **Risk Level** | <Risk Level> |
| **Risk Title** | <Risk Title> | | | | | | | | | | |
| **Capability** | <Capability> | | | | **Sub-Capability ID** | | <Sub-Capability ID> | | **Sub-Capability Name** | <Sub-Capability Name> | |
| **Potential Cause** | <Potential Cause> | | | | | | | | | | |
| *(“…causing…”)* **Potential Event** | <Potential Event> | | | | | | | | | | |
| (“…resulting in…”) **Potential Consequence** | <Potential Consequence> | | | | | | | | | | |
| **RIS** | <RIS> | **RIS Artifact** | | <Artifact(s)> | | **RIS Artifact Element(s)** | | <Artifact Element(s)> | | | |
| **Narrative** | <Narrative> | | | | | | | | | | |

Table . Inherent Risk <Risk ID>: <Risk Title>

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Risk ID** | <Risk ID> | | **Impact** | | <Risk Impact> | | **Likelihood** | | <Risk Likelihood> | **Risk Level** | <Risk Level> |
| **Risk Title** | <Risk Title> | | | | | | | | | | |
| **Capability** | <Capability> | | | | **Sub-Capability ID** | | <Sub-Capability ID> | | **Sub-Capability Name** | <Sub-Capability Name> | |
| **Potential Cause** | <Potential Cause> | | | | | | | | | | |
| *(“…causing…”)* **Potential Event** | <Potential Event> | | | | | | | | | | |
| (“…resulting in…”) **Potential Consequence** | <Potential Consequence> | | | | | | | | | | |
| **RIS** | <RIS> | **RIS Artifact** | | <Artifact(s)> | | **RIS Artifact Element(s)** | | <Artifact Element(s)> | | | |
| **Narrative** | <Narrative> | | | | | | | | | | |

### Residual Risks

“What are the concerns from this risk assessment that arise from closed/mitigated findings or other issues?”

Residual risk is the amount of risk, or danger, remaining in the system after identified weaknesses have been reduced/mitigated. Not all mitigated weaknesses result in residual risk. Residual risk is determined by evaluating the security posture of the system after inherent risks have been reduced by risk controls. Residual risk is monitored through ongoing review of the security posture associated with the system in determining if similar or like weaknesses are identified in subsequent Risk Assessments and can assist in identifying the root causes associated with the weaknesses.

[The following table summarizes the identified residual risks related to each assessed Security Capability; details about these can be found in the various Risk Information Sources and related artifacts listed for each risk. ] OR [This Risk Assessment did not identify any residual risks.]

Table . Residual Risk <Risk ID>: <Risk Title>

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Risk ID** | <Risk ID> | | **Impact** | | <Risk Impact> | | **Likelihood** | | <Risk Likelihood> | **Risk Level** | <Risk Level> |
| **Risk Title** | <Risk Title> | | | | | | | | | | |
| **Capability** | <Capability> | | | | **Sub-Capability ID** | | <Sub-Capability ID> | | **Sub-Capability Name** | <Sub-Capability Name> | |
| **Potential Cause** | <Potential Cause> | | | | | | | | | | |
| *(“…causing…”)* **Potential Event** | <Potential Event> | | | | | | | | | | |
| (“…resulting in…”) **Potential Consequence** | <Potential Consequence> | | | | | | | | | | |
| **RIS** | <RIS> | **RIS Artifact** | | <Artifact(s)> | | **RIS Artifact Element(s)** | | <Artifact Element(s)> | | | |
| **Narrative** | <Narrative> | | | | | | | | | | |

### Inherited Risks

“What are the concerns from this risk assessment that arise from inherited risks, findings, POA&Ms, or other issues?”

Inherited risk is the risk associated with the various controls and functions (or portions thereof) that are implemented by and received from entities other than the system or application being assessed (the “Risk Provider”) – whether internal or external to the organization. Although primary responsibility for mitigating the inherited risk likely does not belong to the system being assessed, the overall risk posture of the system is impacted by the inherited risk and must be considered when determining the overall risk to the system and <Organization>. The system being assessed might be required to take action to mitigate the inherited risk at the assessed system level if the Risk Provider is unable or unwilling to mitigate it on their behalf.

[The following table summarizes the identified inherited risks related to each assessed Security Capability; details about these can be found in the various Risk Information Sources and related artifacts listed for each risk.] OR [This Risk Assessment did not identify any inherited risks.]

Table . Summary of Identified Inherited Security Capability Risks

| Risk ID | Capability | Sub-Capability | Risk Provider | Summary of Inherited Risk | Inherited Risk / POA&M / Finding ID(s) |
| --- | --- | --- | --- | --- | --- |
| <Risk ID> | <Capability> | <Sub-Capability> | <System name of Provider from which the risk(s), finding(s), or POA&M(s) are inherited> | <Summarize the risk(s) described by the risk(s), finding(s), or POA&M(s)> | <POA&M / Finding / Risk ID(s)> |
| <Risk ID> | <Capability> | <Sub-Capability> | <System name of Provider from which the risk(s), finding(s), or POA&M(s) are inherited> | <Summarize the risk(s) described by the risk(s), finding(s), or POA&M(s), finding(s), or risk(s)> | <POA&M / Finding / Risk ID(s)> |

## Summary of Recommendations

“What should we do?”

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

* **Update ISRA:** Brainstorm, document, and analyze what risks the system (and the <Organization> enterprise) faces, beyond pure compliance issues/POA&Ms. Update the ISRA on a regular basis and as new risks are identified, configuration changes are made to the system or environment, new threat information is received, etc. Add and track risks identified by the ACT Risk Assessment process (when applicable). Consider all identified risks in context with each other and document any “meta-risks” that arise from that analysis.
* **Update Personnel Training and Workaids:** The previous ACT Security Assessment identified a significant number of insecure (or potentially insecure) configurations that had been pushed to Production – while those specific compliance issues were quickly addressed, it is not clear what preventative measures have been taken to ensure that similar insecure configurations are not published in the future. Provide appropriate role-based training (for example, in secure coding practices) and update (or create) checklists, workaids, procedures, etc. to ensure that appropriate checks are made prior to publication of new configurations.
* **Update <GRC Tool>:** <GRC Tool> data was out of date at the time of the previous ACT Risk Assessment and remains partially out of date at the time of the current Risk Assessment. Update <GRC Tool> data and ensure that it remains up to date going forward.

# System Information

## Brief Description of System

<Brief description of the system.>

## System Identification and Security Level

Table 5. 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 6. 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 7. 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 8. System Operational Status

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

# Risk Assessment Scope and Methodology

“What was assessed?”

“How was it assessed?”

This section details the scope and execution methodology of the ACT Risk Assessment.

## Risk 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 ACT Risk Assessment:

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

The following tables detail System Information and the Assessment Boundary of this ACT Risk 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 10. ACT Risk Assessment Scope Specification

|  |  |
| --- | --- |
| Risk Information Sources | * A123 Audit * ACT Risk Assessment * ACT Security Assessment * CDM Data Sources * DHS Cyber Hygiene * 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] |

## Risk Assessment Methodology

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

The Assessment Team comprised the following personnel:

Table . Assessment Team Members

| Name | Role | Phone Number | Email Address |
| --- | --- | --- | --- |
| <First Last> | Risk Assessment Lead | <xxx-xxx-xxxx> | <Email Address> |
| <First Last> | Risk Assessor | <xxx-xxx-xxxx> | <Email Address> |

The Assessment Team analyzed data from multiple Risk Information Sources (RIS) (listed in Section 4 below) and identified inherent, inherited, and residual risks to the system and the <Organization> enterprise. The Assessment Team considered the following when identifying risks:

* Applicable security standards (e.g., <Organization> security controls catalog; HIPAA; etc.)
* Applicable <Organization>, <Parent Organization> , and other Federal guidance, directives, and law
* Industry best-practices
* Results of ongoing assessments of other <Organization> systems
* Knowledge of various <Organization> initiatives, events, concerns, etc.
* Historical risk, finding, and security event data
* Subject matter expertise

It should be noted that risk identification and assessment is an inherently qualitative process that is based on many factors that change over time; the risks identified in this report represent a “snapshot in time” of the assessed system and its environment, and they will continue to evolve after publication of this Report.

# Risk Information Sources

“Which Risk Information Sources were used to conduct this Risk Assessment?”

Table 12 provides details about the commonly used Risk Information Sources (RIS) and whether or not they were used to produce this Risk Assessment.

Table . Commonly Used Risk Information Sources

| Risk Information Source | Available? | Utilized? | Provider | Artifact to be Assessed | Artifact Date | Artifact Version | Comment |
| --- | --- | --- | --- | --- | --- | --- | --- |
| A123 Audit | No | No | N/A | N/A | N/A | N/A |  |
| ACT Risk Assessment | Yes | Yes | ISG | SYSTEMNAME ACT Report – Risk Assessment | YYYY-MM-DD | 1.0 | RAR was produced 2 months ago, using a different set of RIS, to assess system risk related to a specific 0-day vulnerability. |
| ACT Security Assessment | Yes | Yes | ISG | SYSTEMNAME ACT Report – Security Assessment | YYYY-MM-DD | 1.0 |  |
| DHS Cyber Hygiene | Yes | No | DHS | N/A | N/A | N/A | ISSO explained that this was performed prior to substantial system upgrades which affect the results. |
| Information System Risk Assessment (ISRA) | Yes | Yes | SYSTEMNAME | SYSTEMNAME Information System Risk Assessment | YYYY-MM-DD | 1.0 |  |
| Inherited POA&Ms | Yes | Yes | XDC | POA&M######## | YYYY-MM-DD | N/A | XDC stated that this POA&M will remain open through next year. |
| Penetration Testing | Yes | Yes | SOC | SYSTEMNAME SOC Penetration Test Results | YYYY-MM-DD | 0.1 |  |
| Privacy Impact Assessment (PIA) | Yes | Yes | SYSTEMNAME | SYSTEMNAME Privacy Impact Assessment | YYYY-MM-DD | 1.0 |  |
| Risk Vulnerability Assessment (RVA) | No | No | N/A | N/A | N/A | N/A |  |
| Security Controls Assessment (SCA) | No | No | N/A | N/A | N/A | N/A |  |
| Security Impact Analysis (SIA) | Yes | Yes | SYSTEMNAME | SYSTEMNAME Security Impact Analysis | YYYY-MM-DD | 1.0 Final |  |
| Self-Assessment | Yes | No | Bogus Security, LLC | N/A | N/A | N/A | Report focused on financial transaction policies, outside scope of this RAR. |
| Technical Review Board (TRB) | Yes | Yes | <Organization> TRB | TRB Approval Package | YYYY-MM-DD | 1.1 |  |
| Vulnerability Scans | Yes | No | SOC | DbProtect Scan Results | N/A | N/A | Scan was run before major update to system, so was determined to be outdated. |
| Yes | Yes | SOC | MITRE SAF Scan Results | YYYY-MM-DD | 0.1 |  |
| Yes | Yes | SOC | Nessus Scan Results | YYYY-MM-DD | 0.1 |  |
| Yes | Yes | SOC | NetSparker Scan Results | YYYY-MM-DD | 0.1 |  |
| Yes | Yes | SYSTEMNAME | SYSTEMNAME Nessus Scan Results | YYYY-MM-DD | 0.1 | System performed this as a one-off for the ACT and does not normally run scans. |

Table 13 provides details about other available RIS that will be used to produce this Risk Assessment.

Table 13. Other Available Risk Information Sources

| Risk Information Source | Utilized? | Source | Artifact Assessed | Artifact Date | Artifact Version | Comment |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

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 14 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 15:

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. |