

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 Plan (RAP)

Record of Changes

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Responsible Author | Description of Change |
| 1.0 | May 30, 2025 | Nate Lee Andrew Bennett Ernie Riviere | Initial release of MITRE ACT templates and work aids. |

**Note to the Author Using this Template:**

This is a *template* for producing a MITRE ACT template tailored to your specific organization. Everything in this template can and should be customized by you to meet your organization’s specific needs and objectives.

Various objects and sections of text throughout the template are highlighted – these are **items that are very likely to require customization**, but you are free and encouraged to **edit the entire document and process** to suit your organization’s needs. By documenting your actual ACT process (including how it deviates from the baseline herein) in this template you are ensuring that your ACT assessments are consistent, repeatable, and can be accurately compared to assessments from other organizations’ implementations of ACT.

Table of Contents

[1. Introduction 1](#_Toc198643212)

[2. System Information 1](#_Toc198643213)

[2.1 Brief Description of System 1](#_Toc198643214)

[2.2 System Identification and Security Level 1](#_Toc198643215)

[2.3 Responsible Organizations 1](#_Toc198643216)

[2.4 System Type Designation and Categorization/Classification 2](#_Toc198643217)

[2.5 System Operational Status 3](#_Toc198643218)

[3. Risk Assessment Scope 3](#_Toc198643219)

[3.1 Boundary Descriptions 3](#_Toc198643220)

[3.1.1 Authorization Boundary Description 3](#_Toc198643221)

[3.1.2 Assessment Boundary Description 6](#_Toc198643222)

[3.2 Risk Assessment Methodology 9](#_Toc198643223)

[3.3 Risk Information Sources 10](#_Toc198643224)

[3.4 Assumptions/Limitations 1](#_Toc198643225)

[3.5 Points of Contact & Assessment Roles 1](#_Toc198643226)

[4. Requirements and Schedule 1](#_Toc198643227)

[4.1 Physical Access and Work Area Requirements 1](#_Toc198643228)

[4.2 Artifact Requirements 2](#_Toc198643229)

[4.2.1 Risk Information Source Outputs 2](#_Toc198643230)

[4.2.2 Tier 1 Artifacts – Minimum Security Artifacts 2](#_Toc198643231)

[4.3 Risk Assessment Estimated Timeline 3](#_Toc198643232)

[5. ACT Assessment Process and Methodology 4](#_Toc198643233)

[5.1 Assessment Phases 4](#_Toc198643234)

[5.1.1 Phase 1: Planning 4](#_Toc198643235)

[5.1.2 Phase 2: Assessment 4](#_Toc198643236)

[5.1.3 Phase 3: Reporting 4](#_Toc198643237)

[5.2 Roles and Responsibilities 4](#_Toc198643238)

[5.2.1 Risk Assessment Lead 5](#_Toc198643239)

[5.2.2 Risk Assessor 5](#_Toc198643240)

[5.2.3 Business Owner 5](#_Toc198643241)

[5.2.4 Cyber Risk Advisor 5](#_Toc198643242)

[5.2.5 Government Task Lead 5](#_Toc198643243)

[5.2.6 Information System Security Officer / Information System Security Manager 6](#_Toc198643244)

[5.2.7 System Owner 6](#_Toc198643245)

[5.3 Risk Assessment Activities 6](#_Toc198643246)

[5.3.1 Risk Information Source Review 6](#_Toc198643247)

[5.3.2 Documentation Review 6](#_Toc198643248)

[5.4 Reporting 7](#_Toc198643249)

[Appendix A. Risk Scoring Methodology 8](#_Toc198643250)

[A.1. Risk Level Assessment 8](#_Toc198643251)

[A.2. Impact Severity 8](#_Toc198643252)

[A.3. Likelihood of Occurrence 9](#_Toc198643253)

# 

# Introduction

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

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

# System Information

## Brief Description of System

<Brief description of the system.>

## System Identification and Security Level

Table 1. System Identification

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

## Responsible Organizations

Table 2. Responsible Organizations

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

## System Type Designation and Categorization/Classification

Table 3. System Type Designation and Categorization/Classification

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

## System Operational Status

Table 4. System Operational Status

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

# Risk Assessment Scope

## Boundary Descriptions

“What will and won’t be assessed?”

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

### Authorization Boundary Description

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

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

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

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

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

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

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

A screenshot of a cell phone

Description automatically generated

Figure . <System Acronym> Official Authorization Boundary Diagram

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

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

A screenshot of a cell phone

Description automatically generated

Figure . <System Acronym> Updated Authorization Boundary Diagram

### Assessment Boundary Description

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

A screenshot of a map

Description automatically generated

Figure . <System Acronym> Assessment Boundary Diagram

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

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

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

The following tables detail System Information and the Assessment Boundary of this HVA 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 3. 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 will analyze data from multiple Risk Information Sources (RIS) (listed in Section 3.3) and identify inherent, inherited, and residual risks to the system and the <Organization> enterprise. The Assessment Team will consider the following when identifying risks:

* Applicable security standards (e.g., <Organization> Security Controls Catalog; <Organization> IS2P2; 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 through this process represent a “snapshot in time” of the assessed system and its environment, and they will continue to evolve after publication of the Risk Assessment Report.

Additional information on Risk Scoring can be found in Appendix A.

## Risk Information Sources

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

Table 4 lists commonly used Risk Information Sources (RIS) and whether they will be used to produce this specific 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/ISSM 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 | CCIC | SYSTEMNAME CCIC 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 | CCIC | DbProtect Scan Results | N/A | N/A | Scan was run before major update to system, so was determined to be outdated. |
| Yes | Yes | CCIC | MITRE SAF Scan Results | YYYY-MM-DD | 0.1 |  |
| Yes | Yes | CCIC | Nessus Scan Results | YYYY-MM-DD | 0.1 |  |
| Yes | Yes | CCIC | 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 5 provides details about other available RIS that will be used to produce this Risk Assessment.

Table . Other Available Risk Information Sources

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

## Assumptions/Limitations

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

* The Assessment Team will have access to all relevant documentation for the system.
* The System Team will provide the Assessment Team with accurate information and evidence at all times.
* Information requested by the Assessment Team will be delivered in a timely manner.
* Artifacts provided by the System Team to the Assessment Team will not contain PII, PHI and/or FTI data.

## Points of Contact & Assessment Roles

The Assessment Team points of contact for the ACT Risk Assessment are listed in Table 6.

Table . Assessment Team Points of Contact and Roles

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

The System Team points of contact for the ACT Risk Assessment are listed in Table 7.

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

Table . System Team Points of Contact and Roles

| Role | Name | Organization | Phone Number | Email Address |
| --- | --- | --- | --- | --- |
| Assessment POC | <First Last> | <Org> | <xxx-xxx-xxxx> | <Email Address> |
| Business Owner | <First Last> | <Org> | <xxx-xxx-xxxx> | <Email Address> |
| Cyber Risk Advisor (CRA) | <First Last> | <Org> | <xxx-xxx-xxxx> | <Email Address> |
| Information System Security Officer (ISSO) / Manager (ISSM) | <First Last> | <Org> | <xxx-xxx-xxxx> | <Email Address> |
| System Owner | <First Last> | <Org> | <xxx-xxx-xxxx> | <Email Address> |

# Requirements and Schedule

## Physical Access and Work Area Requirements

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

OR:

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

## Artifact Requirements

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

### Risk Information Source Outputs

Outputs from the RIS listed in Section 2.3 above must be provided so that the Assessment Team can analyze them and generate the list of overall risks to the system.

### Tier 1 Artifacts – Minimum Security Artifacts

The artifacts in Table 8 provide context to the data pulled from the in-scope RIS and must be provided to assist the Assessment Team in understanding the system authorization boundary, devices in scope, number of components and complexity, etc.

Table . Tier 1 Artifacts – Minimum Security Artifacts

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

## Risk Assessment Estimated Timeline

Table 9 describes the estimated timeline for assessment actions and milestones.

Table . Estimated Timeline for Risk Assessment Actions and Milestones

| Action/Milestone | Description | Date(s) |
| --- | --- | --- |
| Perform Readiness Review | Discuss assessment preparations and ensure tasks (*e.g.*, providing documentation and RIS outputs to the Assessment Team) are on target for completion. |  |
| Deliver documentation, script output, and configuration output to the Assessment Team | Deliver all Artifact requests to the Assessment Team prior to assessment. |  |
| Perform Assessment | Conduct risk assessment activities based on the assessment’s scope. |  |
| Deliver ACT Risk Assessment Report | Put risks identified during the assessment into report format. |  |
| Conduct Review of Report | System personnel and Assessment Team meet to review feedback on Draft Report. System personnel should provide feedback to Assessment Team prior to meeting. |  |
| Deliver updated ACT Risk Assessment Report | Updated based on System Team feedback and finalized. |  |
| Deliver Final Package to <Organization> | Contains all deliverables, work products, artifacts, etc. |  |

# ACT Assessment Process and Methodology

This section outlines the Assessment Team’s assessment methodology to verify and validate that the information system’s Security Capabilities are appropriately implemented RIS and identification of overall risks.

## Assessment Phases

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

### Phase 1: Planning

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

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

* Which **Risk Information Sources** should be included in the assessment, and which should receive the most emphasis.
* Which **system components** (software or hardware) should be included in the assessment, and which should receive the most emphasis.

The Assessment Team will then define agreeable assessment terms and create the ACT Risk Assessment Plan (this document), as approved by <Organization>.

### Phase 2: Assessment

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

* **Information Collection:** thorough research that must be performed against the target system/application before any meaningful assessment can be conducted. Gathered data is analyzed as the assessment proceeds and when the assessment is complete.
* **Enumeration:** activities that provide specific information about assessment targets.

### Phase 3: Reporting

Phase 3, “Reporting”, documents the soundness of the implemented Security Capabilities and consolidates all identified risks into the Risk Assessment Report.

## Roles and Responsibilities

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

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

### Risk Assessment Lead

The Risk Assessment Lead is a member of the Assessment Team and responsible for understanding <Organization> policies, standards, procedures, system architecture, and structures. The Risk Assessment Lead develops the Risk Assessment Plan; assesses the RIS and generates the ACT Risk Assessment Report; and performs all other administrative and management duties for the Risk Assessment.

### Risk Assessor

The Risk Assessor is an optional member of the Assessment Team that supports the Risk Assessment Lead by performing supplementary RIS review and risk identification/analysis.

### Business Owner

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

### Cyber Risk Advisor

The system’s assigned Cyber Risk Advisor (CRA) is responsible for working with the ISSO/ISSM and/or Business Owner to determine the scope of the assessment, and coordinating with the Assessment Team to ensure that their requests are fulfilled and that they are able to complete the assessment. The CRA assists the Assessment Lead with initiating application and system access for the test accounts used during the assessment. At the conclusion of the assessment, the CRA accepts the ACT Report and distributes it to ACT stakeholders.

### Government Task Lead

The Government Task Lead (GTL) is a <Organization> representative for the Application Developer/Maintainer and is responsible for providing technical information to the Assessment Team. During the ACT process, the GTL shall be available for planning sessions, interview with their Application Developer/Maintainer, assisting the Application Developer during application discussions, providing assistance for using the application, and directing the Application Developer/Maintainer to remediate any weaknesses.

### Information System Security Officer / Information System Security Manager

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

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

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

### System Owner

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

## Risk Assessment Activities

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

### Risk Information Source Review

During the assessment phase, the Assessment Team will review the outputs from the various in-scope RIS to identify the overall risks posed to the system and the <Organization> enterprise.

### Documentation Review

Prior to and during the assessment phase, the Assessment Team will review the Tier 1 documents provided by the System Team to understand the context of the RIS data.

## Reporting

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

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 18 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 via the following matrix:

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