

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)™

Assessment Handbook

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.

Logo, MITRE Cyber Solutions Innovation Center.

Motto: Innovating Solutions, Securing the FutureAbout MITRE ACT

MITRE ACT is developed by The MITRE Corporation’s Cyber Solutions Innovation Center (CSIC). The Center brings together world-class expertise and thought leadership to address the extraordinary cybersecurity challenges facing our government, military, and private industry partners.

Leveraging MITRE’s deep knowledge of adversary cyber threats, the Center works with sponsors to architect, assess, and acquire safe, secure, and resilient cyber systems that meet their operational needs. In areas where there are gaps, the Center performs high-impact research and investigations to advance innovative and effective cyber solutions.

For more information about the MITRE Cyber Solutions Innovation Center, visit:  
<https://www.mitre.org/our-impact/mitre-labs/cyber-solutions-innovation-center>

For more information about MITRE ACT visit: <https://act.mitre.org> or email the ACT Development Team at [act@mitre.org](mailto:act@mitre.org).

Acknowledgements

MITRE ACT has been developed over many years with the involvement of many individuals across government and industry. The primary authors – Andrew Bennett, Ernie Riviere, and Nate Lee – wish to thank all of their colleagues who reviewed drafts and assisted in the production of ACT, especially: Andy MacBrien, Anthony Porcelli, Belinda Edwards, Brett Kreider, Jim Bielski, Mike Gazdus, Naqi Sayed, Rick Swihart, Robert Fout, and Stefan DeShazo.

The authors also gratefully acknowledge and appreciate the comments and contributions made by various government agencies, private organizations, and individuals in providing direction and assistance in the development of this risk-based decision-making framework.

Table of Contents

[1. Introduction 1](#_Toc198587411)

[1.1 Handbook Purpose 1](#_Toc198587412)

[1.2 How to Use This Handbook 1](#_Toc198587413)

[1.3 Overview of ACT Framework and Methodology 2](#_Toc198587414)

[1.3.1 Background 2](#_Toc198587415)

[1.3.2 The ACT Difference 3](#_Toc198587416)

[1.3.3 Emphasis on Clear Communications 4](#_Toc198587417)

[1.3.4 Security Capabilities 4](#_Toc198587418)

[1.3.5 Risk Information Sources 6](#_Toc198587419)

[1.3.6 Core Controls 6](#_Toc198587420)

[1.3.7 Assessment Types 7](#_Toc198587421)

[1.3.8 Risk Scoring Methodology 10](#_Toc198587422)

[1.3.9 Personnel Roles and Responsibilities 13](#_Toc198587423)

[1.3.10 Safeguarding <Organization> Data 15](#_Toc198587424)

[1.3.11 Compliance with Standards, Policies, and Procedures 16](#_Toc198587425)

[2. ACT Process (Risk Assessment and Security Assessment) 18](#_Toc198587426)

[2.1 Phase 1: Planning 19](#_Toc198587427)

[2.1.1 Start Assessment 20](#_Toc198587428)

[2.1.2 Conduct Preliminary Discussion 21](#_Toc198587429)

[2.1.3 Review Tier 1 Artifacts 23](#_Toc198587430)

[2.1.4 Develop Assessment Plan 24](#_Toc198587431)

[2.1.5 Conduct Assessment Plan Review Meeting 27](#_Toc198587432)

[2.1.6 Conduct Readiness Review Meeting 29](#_Toc198587433)

[2.1.7 Assessment Team Preparation 29](#_Toc198587434)

[2.1.8 Notify Technical Writer/Editor of Key Dates for Report 32](#_Toc198587435)

[2.1.9 Deliver Updated Assessment Plan 32](#_Toc198587436)

[2.2 Phase 2: Assessment 33](#_Toc198587437)

[2.2.1 Security Assessment Lead 35](#_Toc198587438)

[2.2.2 Risk Assessment Lead 38](#_Toc198587439)

[2.2.3 Risk Assessor 40](#_Toc198587440)

[2.2.4 Management and Operations (M&O) Assessor 41](#_Toc198587441)

[2.2.5 Application Assessor 48](#_Toc198587442)

[2.2.6 Database Assessor 54](#_Toc198587443)

[2.2.7 Operating System Assessor 58](#_Toc198587444)

[2.2.8 Virtualization Assessor 62](#_Toc198587445)

[2.2.9 Mainframe Assessor 66](#_Toc198587446)

[2.2.10 Network Assessor 70](#_Toc198587447)

[2.2.11 Cloud Assessor 74](#_Toc198587448)

[2.2.12 Privacy Assessor 78](#_Toc198587449)

[2.3 Phase 3: Reporting 81](#_Toc198587450)

[2.3.1 Develop Assessment Report, Findings File, and Risks File 81](#_Toc198587451)

[2.3.2 Conduct Assessment Report Review Meeting 82](#_Toc198587452)

[2.3.3 Update Assessment Report, Findings File, and Risks File 83](#_Toc198587453)

[2.3.4 Upload Assessment Report, Findings File, and Risks File to <Storage Location> 83](#_Toc198587454)

[2.3.5 Create and Deliver Final Package 83](#_Toc198587455)

[2.4 Process Improvement Follow-Up 86](#_Toc198587456)

[3. Attachments 87](#_Toc198587457)

[4. Acronyms 1](#_Toc198587458)

# Introduction

MITRE Adaptive Capabilities Testing (ACT)™[[1]](#footnote-2) is a security and risk assessment framework that implements risk-based decision-making by focusing on how mission or business capabilities are impacted by the full context of available risk information – not merely by compliance with specific requirements.

ACT implements a process that is efficient, cost-effective, flexible, repeatable, and measurable. It helps organizations meet the objectives of the NIST *Risk Management Framework* (RMF) and similar processes (*e.g.*, the Department of Defense RMF). ACT can serve as the primary input to Authorization to Operate (ATO) decisions[[2]](#footnote-3). Compared to compliance-oriented assessments (such as Security Controls Assessment (SCA)), ACT is:

* **Risk-driven** rather than **compliance-driven**: ACT **focuses on risk** identification and analysis at the Capability-level and **de-emphasizes technical findings** and compliance with Controls and other technical requirements.
* **Capability-oriented** rather than **control-oriented**: Capabilities state **objectives** while Controls/requirements state specific **implementation requirements** that *might* help meet those objectives.
* Based on multiple **Risk Information Sources (RIS)**: ACT considers **all available risk data** at the time of the assessment, not just the current state of compliance with Controls/requirements.
* More **understandable** and **actionable**: ACT adds context, brings conversation to a higher level, and focuses on helping the reader **determine what *should* be done**.

This Handbook expands upon these principles.

## Handbook Purpose

The purpose of this document is to guide each ACT Assessment Team member through the processes required to successfully execute an ACT Security Assessment and/or an ACT Risk Assessment in support of the ATO process. It aims to provide enough explanation and detail to clearly explain the processes of executing these assessments while allowing the Assessment Team plenty of leeway to adjust the process to suit the situation.

## How to Use This Handbook

This handbook details the Security Assessment process in detail and notes where there are deviations for the separate Risk Assessment process. Usually if a Security Assessment is being conducted then a Risk Assessment will also be conducted and so the entirety of this Handbook will apply. If *only* one of these assessment types is being performed then only certain portions of the Handbook apply.

When conducting a Risk Assessment (either stand-alone or in conjunction with a Security Assessment), the Risk Assessment Lead should use the following sections and corresponding subsections:

* 1 Introduction
* 2.1.1 Start Assessment
* 2.1.2 Conduct Preliminary Discussion
* 2.1.3 Review Tier 1
* 2.1.4 Develop Assessment Plan
* 2.1.5 Conduct Assessment Plan Review Meeting
* 2.1.8 Notify Technical Writer/Editor of Key Dates for Report
* 2.1.9 Deliver Updated Assessment Plan
* 2.2.2 Risk Assessment Lead
* 2.2.3 Risk Assessor
* 2.3 Phase 3: Reporting
* 2.4 Process Improvement Follow-Up

## Overview of ACT Framework and Methodology

This section provides an overview of the ACT framework and methodology.

### Background

An organization’s Security Assessment and Authorization (SA&A) Program protects the security and privacy posture of their systems throughout the system development lifecycle. Mature SA&A programs require all systems to undergo a comprehensive risk assessment before receiving ATO, but without a comprehensive and flexible risk-based decision-making framework it can be difficult for SA&A programs to satisfactorily meeting the risk assessment requirement. Many existing SA&A programs are based primarily on the SCA process (which is compliance-oriented rather than risk-oriented), which results in the following problematic authorization workflow:

* An SCA identifies some number of low-level, highly technical areas of non-compliance with specific <Organization’s Controls Catalog> Controls (“Findings”).
* These highly technical SCA Findings are then provided (with little or no context) to less-technical, higher-level decision-makers and leaders.
* Those decision-makers are expected to determine, on their own, what to do about the SCA Findings.
* Without a formal framework for appropriately **understanding the meaning** of these SCA Findings **in context** and **deciding whether or not they should comply with the <Organization’s Controls Catalog> Controls**, decision-makers are instead implicitly encouraged to **blindly comply** with the <Organization’s Controls Catalog> Controls to close the SCA Findings for ATO purposes.
* Consequently, SCA Findings are closed through potentially unnecessary and costly work, the actual risk posture of the system remains poorly understood throughout the ATO process, and the cycle continues again the next year with the next SCA.

### The ACT Difference

Diagram

AI-generated content may be incorrectA Venn diagram illustrating risk-based decision-making in cybersecurity, titled “What should I do?” at the center. The diagram has three overlapping circles:
	1.	Green circle (top) – Labeled “Risk-Based Decision Making: What SHOULD I do?” Includes proactive (acquisition, assessment, 0-days) and reactive (assessment, incident response) actions. Asks: “Which attacks pose the highest risk?” and “Which defenses reduce which risks?”
	2.	Red circle (left) – Labeled “Attacks: What CAN the attacker do?” Cites methods like MITRE ATT&CK and penetration testing. Asks: “How can attacker compromise defender?”
	3.	Blue circle (right) – Labeled “Defenses: What CAN the defender do?” Refers to MITRE DEFEND, SCA, and others. Asks: “How can defender thwart attacker?”

The overlapping center of all three circles highlights integrated analysis to support cybersecurity decisions..

Figure . ACT Decision-Making Framework

The ACT framework directly addresses these deficiencies by reimplementing a streamlined SCA as one of many *Risk Information Sources* (“RIS”, see Section 1.3.5) called the *ACT Security Assessment*, and by implementing the *ACT Risk Assessment* which evaluates the current results of *all* available and relevant *Risk Information Sources*. Risk Information Sources are (as the name implies) various sources of information about the system and its context that help describe the risk-posture of the system. The ACT Risk Assessment identifies the risks that arise from these RIS’s in aggregate and describes their impact on various enterprise-level Security Capabilities (which are *understandable high-level objectives* that the Controls *might* help a system achieve, described in Section 1.3.4).

This *contextual* analysis of risk arising from the various RIS provides higher-level analysis of the *actual security impact* of low-level implementation details (such as Control-oriented Findings) *in aggregate*, and shifts the conversation from a narrow focus on *compliance* to a broader focus on *risk-based decision making*. This *empowers and encourages* decision-makers to choose to comply with a Control *or* to make a risk-based decision to request to remain non-compliant, and provides the authorizing official (AO) with the information needed to determine whether or not to accept the identified risks and to grant an ATO.

**In summary:** **where SCA *by itself* encourages blind compliance with Controls, ACT encourages and equips stakeholders and decision-makers to understand the security objectives (Capabilities) in context and to make informed risk-based decisions about whether or not to comply with a Control.**

The ACT assessment framework is being actively developed to support various transformative initiatives. ACT is designed to be agile and extensible, and it will evolve over time.

### Emphasis on Clear Communications

*“I have only made this letter longer because I have not had the time to make it shorter.”*  
– Blaise Pascal, The Provincial Letters

The ACT assessment framework emphasizes the need for clear, accurate, unambiguous documentation and communications (both verbal and written) that “tell the appropriate story” that each audience needs to hear in a comprehensive yet concise manner. An informal description of this emphasis is “*hard writing makes easy reading*”: the authors of an ACT document or communication must put in the “hard” work of communicating well so that the reader has an “easy” time of understanding it and gleaning from it what they need. All ACT deliverables and artifacts (such as Assessment Plans, Assessment Reports, and Meeting Notes, definitions of each assessed system’s authorization boundary and assessment boundary, etc.) must be clear, accurate, unambiguous, and “easy” to use by each intended audience member of the deliverable. Questions to ask oneself while writing include:

* Who will read what I am writing?
* What do they need to do with it?
* Do they need to use it to brief someone else?

If the reader becomes confused or isn’t easily getting what they need, they are likely to either become frustrated and stop reading, or (worse) glean from the deliverable a wrong understanding and a negative impression of the system, the Assessment Team, the ACT program, or the <Organization Information Security Group>. The author of any ACT document should constantly consider how she might be able to tell the “story” in a clear and actionable manner. Would a picture, which is “worth a thousand words”, help? Would a table or a bulleted list present data more clearly than a paragraph? ACT emphasizes the necessity of the Assessment Team putting in the effort required for clear, accurate, and unambiguous writing so that the audience understands what they need with minimal effort.

### Security Capabilities

<Organization> has identified a set of Cybersecurity Capabilities that guide and focus implementation of security Controls and other security requirements to facilitate better understanding of the maturity of <Organization> systems’ security and privacy risk postures. Drawing inspiration from both the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) and National Institute of Standards and Technology (NIST) Interagency Report (NISTIR) 8011 models, the <Organization> security capabilities address a series of attack steps outlined in NISTIR 8011.

Controls are technical implementation requirements and are the level at which <Organization> analyzes and discusses how a system is or is not complying with those requirements. Capabilities are overall objectives, and are the level at which <Organization> analyzes and discusses what the system’s compliance or non-compliance *means* – is the system “secure enough”, and should <Organization> address the system’s non-compliance?

The Capabilities are listed in the table below and are detailed in the ACT Capabilities Mapping spreadsheet (see Section 3 *Attachments*).

Table . <Organization> Cybersecurity Capabilities

|  |  |
| --- | --- |
| Short Name | Full Name |
| BEHAVE | Manage Behavioral Expectations |
| 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

Each Capability is further broken down into Sub-Capabilities that map to <Organization’s Controls Catalog> security Controls. Each Sub-Capability can be mapped to multiple <Organization’s Controls Catalog> Controls, and each <Organization’s Controls Catalog> Control can be mapped to multiple Sub-Capabilities. This model reveals and leverages the interactions and interdependencies between Security Controls, gains new efficiencies in the assessment process (since assessment of a single Control informs multiple Sub-Capabilities), and provides more actionable insight into <Organization>’ security posture both at the system level and across the organization. The Sub-Capabilities and their Control mappings are provided in the ACT Capabilities Mapping spreadsheet (see Section 3 *Attachments*).

### Risk Information Sources

ACT implements an intelligent form of risk assessment that integrates results from available Risk Information Sources (RIS’s). The ACT Risk Assessment includes previous and ongoing audits and assessments (including ACT-related activities) as well as data available from the CDM program of the <Organization’s SOC/NOC>. The Assessment Team is required to use all available and appropriate RIS’s when conducting an ACT Risk Assessment. It is likely that many systems will be covered by only a subset of the approved RIS types; the Assessment Team will work with the system’s Cyber Risk Advisor (CRA) and (if appropriate) the Government Task Lead (GTL) and follow their guidance to determine which RIS’s to use for each Risk Assessment to provide as comprehensive of a view as possible of the system’s risk(s).

At the time of publication of this Handbook, the commonly available <Organization> RIS’s include:

* A123 Audit
* ACT Risk Assessment
* ACT Security Assessment[[3]](#footnote-4)
* Continuous Data Monitoring sources
* Executive Orders, Department Memos, *etc*.
* Information System Risk Assessment (ISRA)[[4]](#footnote-5)
* Inherited POA&M[[5]](#footnote-6)
* News and World Events
* Penetration Testing[[6]](#footnote-7)
* Real-time Sensor Data
* Risk Vulnerability Assessment (RVA) (for HVA systems)
* Security Controls Assessment (SCA)
* Self-Assessment
* Technical Review Board (TRB)
* Vulnerability Assessment
* Vulnerability Scan

The ACT Assessment Team will incorporate any available RIS’s into the Risk Assessment process, including RIS’s not included in this list.

### Core Controls

The Core Controls are the set of <Organization’s Controls Catalog> Controls that help protect <Organization> systems from the **highest risk** **vulnerabilities**, and therefore they are assessed as part of every ACT. The Core Controls are determined by <Organization> from a complex set of inputs and are redetermined on an as-needed basis. Because these controls pose the highest risk to <Organization> at the time of their publication, the ACT process *prioritizes* assessment of these Controls in the Security Assessment. This means that, while all other in-scope controls are assessed as well, the Core Controls undergo *enhanced assessment and review*, details of which are determined by the ACT Team on a case-by-case basis.

### Assessment Types

There are two types of assessment that can be performed under ACT: **Risk Assessment** and **Security Assessment**.

#### Risk Assessments

The goal of the ACT Risk Assessment is to provide a mostly plain-language report that quickly and easily informs a lay person about the overall health of a system. The report is intended to empower the <Organization> business owner with insights and the information needed to determine an action plan and inform the business owner what should be fixed first and why that is important. It is also the focal point of the ATO process, cutting through the technical jargon of the various low-level security assessments and other sources of low-level risk information to tell the Authorizing Official and other readers “*what it all means.*” The Risk Assessment is not focused on detailing low-level vulnerabilities (*e.g.*, “findings” at the level of <Organization’s Controls Catalog> Controls), but rather on “connecting the dots” between different seemingly disconnected Risk Information Sources by using the high-level Security Capabilities as the common set of requirements between them. The Risk Assessment is successful when it enables risk-based decision making by clearly considering the various Risk Information Sources *together* and explaining the meaning and impact of the various Risk Information Sources on the system’s risk posture *together*.

The ACT Risk Assessment implements a meta-risk-analysis of *all available RIS’s* for the system being assessed. A Risk Assessment is usually performed each time a Security Assessment is performed and may also be performed independently of a Security Assessment on an as-needed basis. The Risk Assessment analyzes the available RIS (*usually* including the Control compliance data from an ACT Security Assessment). The various RIS’s give low-level details about compliance, configuration, etc. (the *“what”*); the intent of the Risk Assessment is to explain in plain language what the low-level details mean from a risk perspective – to answer the question, “*So what?*” Risk Assessments can be performed for individual systems or groups of systems (including the entire <Organization> enterprise).

##### Risk Categories

The ACT framework divides Risks into three (3) categories:

* **Inherent** risks are those that arise directly from unmitigated findings (including open Plan of Action and Milestones (POA&M)
  + Example: A system has two findings related to the password mechanism and three findings related to user account expiration; these might result in one risk that explains that the identification and authentication (I&A) mechanism is weak.
* **Residual** risks are those that arise indirectly, either from already-mitigated findings or from some source other than technical findings.
  + Example:The system mitigated the I&A-related findings mentioned above – although those findings are now “closed” and the *Inherent* risk has been addressed, there may be a *Residual* risk that points out that there’s something wrong with the development processes, because those weaknesses should not have been present in the first place.
* **Inherited** risks are those that are received through inheriting security controls from another system. Any open POA&Ms or risks for a system that the system is inheriting from have an impact on the system’s risk posture; ACT considers this and informs the system of the impact their control providers have on them.
  + Example: The datacenter hosting the system has an open POA&M related to failure to provide adequate physical access control to the datacenter floor; since the datacenter is a separate FISMA-accredited system, this finding cannot be closed or mitigated by the system being assessed, so the system inherits the risk associated with this POA&M from the other system.

#### Security Assessments

The goal of the ACT Security Assessment is to determine the correctness and reliability of the assertions made about <Organization’s Controls Catalog> compliance by the system’s documentation and personnel by reviewing documentation, interviewing personnel, and exercising the system at some acceptable level of detail. Any non-compliances or inconsistencies found are documented as “findings” (*i.e.*, a “finding of non-compliance”). An ACT Security Assessment is structurally and functionally similar to the legacy SCA process: using many of the same tools and techniques, the Security Assessment determines system compliance with each <Organization’s Controls Catalog> Control and documents non-compliance in the form of technical, management, and operational findings. It involves low-level technical testing, interviews, and review of various documents and artifacts, but it leverages existing RIS to minimize new technical testing. Security Assessments are one of the RIS considered in a Risk Assessment.

##### Vulnerability Assessment vs. Penetration Testing

The type of technical testing performed during an ACT Security Assessment comprises 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, Vulnerability Assessment *looks for* vulnerabilities in a system and reports *potential* exposures, while Penetration Testing *exploits* vulnerabilities and other weaknesses in the architecture of the system or network to *determine the degree* to which a malicious attacker can gain unauthorized access to the system. However, the Vulnerability Assessment stops once a determination is made that a vulnerability could (or could likely) be exploited – the Assessors performing a Vulnerability Assessment do not attempt to fully exploit and escalate the vulnerabilities (as Penetration Testers would).

##### Security Assessment Categories

<Organization> defines several categories of Security Assessment:

1. **Comprehensive Scope:** All Capabilities/Sub-Capabilities and <Organization’s Controls Catalog> Controls are included in the Security Assessment.
2. **Tailored Scope:** Only a specified subset of Capabilities/Sub-Capabilities and/or <Organization’s Controls Catalog> Controls are included in the Security Assessment.
3. **Application-Only:** Similar in concept to “a software program downloaded or provided on CD”. Includes only application code/logic and database *instances* that are intended to directly perform <Organization> work. Does not include “supporting” components such as operating systems, database *platforms*, network devices or configurations, etc. For example, Application-Only includes the *tables and data* in the database, but does not include the *database itself* (*e.g.*, the specific installation of Oracle).
4. **Infrastructure-Only:** Similar in concept to “stuff that exists to enable *another* system to operate and perform <Organization> work”. Includes components that are intended to support the operation of an application or system – for example, includes operating systems, database *platforms*, network devices or configurations, etc. Does not include application code and database *instances* that are intended to directly perform <Organization> work.
5. **Application + Infrastructure**: Similar in concept to “a complete standalone system”. Includes components covered by both “Application-Only” and “Infrastructure-Only” in a single system/authorization boundary/assessment. A typical example of this type of assessment is a system that includes within its authorization boundary an Application, a database server, and an operating system.
6. **High Value Asset (HVA):** As defined in the DHS publication *Securing High Value Assets[[7]](#footnote-8)*, HVAs are: “*Federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States’ national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people.*”

##### Levels of Testing Rigor

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

Table . Levels of Testing Rigor A table used for evaluating levels of cybersecurity assessment findings across different criteria. The table is divided into several rows and columns:

Column Headings (left to right):
	•	Category / Type of Finding
	•	Notes
	•	Level 0: Non-Evaluable
	•	Level 1: Assertion Awareness
	•	Level 2: Basic Conditions Verified
	•	Level 3: Advanced Conditions Verified
	•	Level 4: Test
	•	NIST 800-53 Assessment Methods

Row Categories (top to bottom):
	•	Title (e.g., “Typical Use”)
	•	Question Answered
	•	Goals Achieved
	•	Assertion Verified (with subcategories: Interview, Test Results, Pen Test Exploits, Code Controls)
	•	Documentation (with subcategories: Design/Architecture, Config/Setup/Policy, Test Results)
	•	Tools Used (with subcategories: Static Analysis, Dynamic Analysis, Maintenance)
	•	System Access Needed

Each row maps the progression of cybersecurity assessment maturity from Level 0 to Level 4 with checkmarks (✓) showing which levels apply to each method or tool. For example:
	•	“Assertion Verified via Test Results” applies from Level 2 to Level 4.
	•	“Pen Test Exploits” are marked only at Level 4.
	•	“Static Analysis Tools” are applicable from Level 1 through Level 3.

The rightmost column (orange/red background) indicates which combinations of NIST 800-52 Assessment Methods (Examine, Interview, and Test) should be used to assess each category.

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

### Risk Scoring Methodology

A Risk Level value must be assigned to each risk and finding to provide a guideline by which to understand its procedural or technical significance.

#### Risk Level Assessment

Each risk and finding must be assigned a Risk Level value of “Critical”, “High”, “Moderate”, or “Low” as defined in Table 3 below. This rating is, in effect, an assessment of the priority for addressing each risk and finding. Note that the Risk Level for a *finding* is calculated *in isolation*, while the Risk Level for Risks is calculated *in context of all available Risk Information Sources.* **The Risk Level assigned to a Finding should not be used as the sole basis of risk-based decision-making.**

Table 3. Risk Level Definitions

|  |  |
| --- | --- |
| **Rating** | **Definition of Impact Rating** |
| Low | Exploitation of the vulnerability will cause minimal impact to <Organization> 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 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 <Organization>. |
| High | Exploitation of the vulnerability will cause substantial harm to <Organization> business processes. Significant political, financial, and legal damage is likely to result. |
| Critical | Exploitation of the vulnerability will cause catastrophic adverse effects to <Organization> 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, which is based on the latest guidance from <Organization Information Security Group>.

Table 4. 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 |

#### Impact Severity

For each risk and finding, a determination must 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 5. 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, <Organization>, and/or notable loss of confidence in the ability for <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 <Organization> public programs and services. |
| Critical | * Might be expected to have multiple severe or catastrophic adverse effects on <Organization> operations, organizational assets, individuals, other organizations, or the Nation. * Might cause damage to the reputation of system management, <Organization>, and/or notable loss of confidence in the ability for <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 <Organization> public programs and services. |

#### Likelihood of Occurrence

For each risk and finding, a determination must 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 6. 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. |

### Personnel Roles and Responsibilities

The following roles are essential to the successful execution of an assessment:

* **Government Task Lead (GTL):** <Organization> staff, assigned to the <Organization Information Security Group>, designated to oversee and facilitate the ACT process.
* **Cyber Risk Advisor (CRA):** <Organization> staff, assigned to the <Organization Information Security Group>, who coordinates with the Business Owner and ISSO/ISSM to obtain a system’s Authorization to Operate (ATO).
* **Business Owner (BO):** <Organization> business unit personnel responsible for the system as a whole.
* **Information System Security Officer (ISSO):** <Organization> business unit personnel responsible for the security of the system, reports to the Business Owner.
* **Security Assessment Lead:** Assessment Team member (usually a <Organization> contractor) who leads an ACT Security Assessment team that qualifies as an independent[[8]](#footnote-9) third-party assessor. The Security Assessment Lead:
  + Manages Security Assessment scope, schedule, and resources.
  + Assembles and manages the Security Assessment team and their performance.
  + Manages the production and delivery of all Security Assessment Team communications, artifacts, and deliverables to meet all <Organization> requirements for clarity, accuracy, legibility, content, and quality.
  + Is responsible for delivering successful Security Assessment outcomes.
* **Risk Assessment Lead:** Assessment Team member (usually a <Organization> contractor) who leads an ACT Risk Assessment team that qualifies as an independent third-party assessor. The Risk Assessment Lead:
  + Manages Risk Assessment scope, schedule, and resources.
  + Assembles and manages the Risk Assessment team and their performance.
  + Manages the production and delivery of all Risk Assessment Team communications, artifacts, and deliverables to meet all <Organization> requirements for clarity, accuracy, legibility, content, and quality.
  + Is responsible for delivering successful Risk Assessment outcomes.
* **ACT Assessors:** These are qualified subject matter experts (usually <Organization> contractors) who focus on evaluating a specific practice area (such as Management and Operations (M&O) or Privacy) or technology (such as network, operating systems, web applications, mainframes, databases, etc.) and serve as members of an ACT Security Assessment or ACT Risk Assessment team.
* **Tech Editors, Quality Assurance SMEs, etc.:** Support personnel (usually <Organization> contractors) who assist the Assessment Teams with producing and delivering consistent, clear, unambiguous, professional deliverables and communications that meet the various requirements laid out by <Organization> in the ACT contract Statement of Work (SoW) or other <Organization> guidance or directives.

#### Personnel Qualifications

All personnel that perform or assist with Risk Assessments, Security Assessments, editing, quality assurance, or project/program management work must meet the following qualifications (as applicable):

* Have an acceptable number of years of relevant professional experience in the Information Security / Cyber Security field (refer to the ACT contract SoW for the specific requirement).
* Perform security assessment activities that meet both industry best practices and <Organization> expectations.
* Comply with applicable <Organization> and federal security standards, policies, and procedures.
* Understand the type of software, operating systems, and infrastructure used by the system that is undergoing security testing to ensure that the system is adequately tested and that any security vulnerabilities identified are appropriately addressed.
* Possess or obtain current professional certifications commensurate with the duties they will perform in their assigned assessment role(s) (*e.g.*, PMP[[9]](#footnote-10), CISSP[[10]](#footnote-11), CISA[[11]](#footnote-12), CISM[[12]](#footnote-13), SANS[[13]](#footnote-14) GSNA[[14]](#footnote-15), etc.).
* Communicate complex technical and procedural topics clearly and succinctly in both verbal and written communications to a large variety of different stakeholders with varying technical knowledge, and must be ensure that all communications, artifacts, and deliverables they produce meet all <Organization> requirements for clarity, accuracy, legibility, content, quality, etc.

In addition, personnel filling the Security Assessment Lead or Risk Assessment Lead roles must:

* Possess demonstrable and deep knowledge of <Organization> Security Policies, Procedures, Standards, and Methodologies.
* Possess a technical background in a wide array of technologies, network devices, hardware, and software, so that they understand and can discuss Infrastructure and Application vulnerabilities if discovered during an ACT engagement.
* Have demonstrable experience successfully leading SCA or ACT assessments at or for a federal agency or organization.
* Communicate clearly and succinctly in English in both verbal and written communications.

#### Team Makeup

Each Risk Assessment and Security Assessment team must consist of an ample number of Assessors to adequately cover all the technologies, devices, databases, interviews, and documentation evaluations involved in the assessment. Table 7 lists which specific Assessor roles (and approximately how many of each) might be required on a typical assessment. Section 2.2 *Phase 2: Assessment* explains these roles and their assessment responsibilities in detail.

Table 7. Typical Assessment Team Makeup Per Assessment

| **Role** | **Assessment Type** | **Requirement** | **Typical #** |
| --- | --- | --- | --- |
| Risk Assessment Lead | Risk | Mandatory | 1 |
| Risk Assessor | Risk | If needed | Varies |
| Security Assessment Lead | Security | Mandatory | 1 |
| Management and Operations (M&O) Assessor | Security | Mandatory | 1 |
| Application Assessor | Security | Mandatory | 2 to 4 |
| Database (DB) Assessor | Security | If needed | 1 |
| Operating System (OS) Assessor | Security | If needed | 1 to 2 |
| Virtualization Assessor | Security | If needed | 1 |
| Network Assessor | Security | If needed | 1 |
| Cloud Assessor | Security | If needed | 1 |
| Privacy Assessor | Security | If needed | 1 |
| Mainframe Assessor | Security | If needed | 1 |
| Others as required | Risk or Security | If needed | Varies |

Each Assessor must be assigned to at least one of the Assessor roles listed in Table 7 and these assignments must be listed in the appropriate Risk Assessment Plan and/or Security Assessment Plan as directed in the appropriate templates. If the Risk Assessment Lead or Security Assessment Lead wishes to assign one person to multiple assessment roles on a single assessment, or to roles on multiple simultaneous/overlapping assessments of different systems, the Lead must obtain approval from <Organization> before such assignment. <Organization> will only allow multiple assignments if the Lead can ensure (to the GTL’s satisfaction) that each team member has ample time to execute all their responsibilities on each assessment to the satisfaction of <Organization> and in accordance with all <Organization> and industry standards and best practices. <Organization> will also only approve an Assessment Plan if in <Organization>’s opinion an adequate number of personnel have been assigned to the assessment.

### Safeguarding <Organization> Data

All personnel and organizations have a duty to safeguard all assessment data from unauthorized access. Because the loss or disclosure of ACT Security Assessment and Risk Assessment data could be particularly damaging to <Organization> enterprise-wide, the Assessment Teams should work closely with the GTL and system CRAs to ensure that assessment data is handled appropriately for each system’s risk posture.

#### Non-Disclosure

Assessment Team members must treat all <Organization> data as confidential and shall disclose information collected during the ACTs only to authorized <Organization> and designated Assessment Team personnel. The Assessment Team must add appropriate markings to all documents, as dictated by the GTL or COR.

#### Secure Storage

The Assessment Team must protect all assessment data from unauthorized access and secure it according to the requirements of <Organization Applicable IS policies and standards> and <Organization’s Controls Catalog>.

#### Secure Communications

Many sensitive documents and data must be shared between the Assessment Team and the System Team during the ACT process. Whenever feasible, the Assessment Team should transfer sensitive files and documents via the <Organization’s Secure File Transfer System>. When use of <Organization’s Secure File Transfer System>is not feasible, the Assessment Team must implement and use an approved mechanism for secure file transfer over non-<Organization> networks (for example, via email that includes senders or recipients that are not using @<Organization Email Domain> email addresses). <Organization> allows sensitive documentation to be emailed via .zip files encrypted via 128-bit (or higher) AES (Advanced Encryption Standard); however, many documents exceed the file size limitation of the <Organization> email server and <Organization> has found that many external stakeholders’ email systems may strip .zip files from the email. Any encryption mechanism (secure file transfer server, WinZip/SecureZIP, etc.) used or provided by the Assessment Team must be FIPS 140-3 (or 140-2) validated and be operating in the FIPS-approved mode of operation.

### Compliance with Standards, Policies, and Procedures

The ACT framework complies with federal standards, policies, and procedures, including FISMA, the security-related areas as established and specified by the NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Federal Information Systems and Organizations,*[[15]](#footnote-16) and the mandatory and non-waiverable Federal Information Processing Standards (FIPS) 200 *Minimum Security Requirements for Federal Information and Information Systems*.[[16]](#footnote-17)

<Organization> has developed and published the <Organization’s Controls Catalog>,[[17]](#footnote-18) *<Organization> Information Systems Security and Privacy Policy (IS2P2)*,[[18]](#footnote-19) and *<Organization> Technical Reference Architecture (TRA)*.[[19]](#footnote-20) The <Organization’s Controls Catalog> contains a broad set of required security controls based on NIST SP 800-53 and NIST 800-63-3*, Digital Identity Guidelines,*[[20]](#footnote-21) as well as additional standards established by <Organization> policies, procedures, and guidance; other federal and non-federal guidance resources; and industry best practices. The controls outlined in these policies must be implemented to protect <Organization> information and <Organization> information systems.

# ACT Process (Risk Assessment and Security Assessment)

The ACT assessment process is divided into three phases: Planning, Assessing, and Reporting. Standardized templates have been created for the associated documentation and artifacts as supporting evidence per phase. The complete list of the templates and guidance can be found in Section 3 *Attachments*. The following sub-sections and figure below provide further detail for each of the phases, referencing guidance, artifacts, and process steps to be followed. Figure 2 provides an overview of the tasks for each phase and shows a font color difference between Security and Risk assessment tasking. **The first three bullets within the Assessment Phase column are for the Security Assessment task.**



Figure . Assessment Phases

## Phase 1: Planning

The **Planning phase** for both Security Assessments and Risk Assessments collects information and produces inputs to the ACT Assessment Plan, which lays the foundation for the rest of the process. During this phase, it is necessary to obtain as much information as possible about the system by identifying the appropriate parties involved, defining the controls to be tested, and documenting which components of the system are to be assessed. Coordination conference calls are held to conduct an ACT preliminary discussion, to review the ACT Assessment Plan and identify any changes required prior to the assessment, discuss application testing, and to determine the readiness of the system for ACT. Additional logistical activities are performed such as educating the system’s personnel about the assessment methodology, obtaining test accounts (credentials username/password, and test data), conducting a live demonstration of the application, agreement on testing location(s) and time, and how Findings and other information will be communicated. Risk Assessments will follow the same plan as Security Assessments as they are often conducted in parallel. Timeframes for Risk Assessments that are conducted independently from Security Assessments are still being developed.

A workflow diagram of Phase 1.

Figure . Phase 1: Planning

<Organization> uses the *<Organization> System Security Level Definitions* to categorize systems as *Low*, *Moderate*, or *High*. As the security level increases, so too must the level of testing rigor and comprehensiveness. The Security Assessment Lead must account for the security level of the system in their planning and test execution, ensuring that Assessment Team personnel and management select and execute proper levels of rigor and completeness for each system.

An important aspect of planning is to ensure the clear definition of the full scope of every assessment and that both authorization and assessment boundaries are clearly understood and documented. <Organization> systems often rely on other Business Owners to provide security protections; therefore, it is important to assess these relationships and plan testing activities accordingly.

It is also very important to work with the system team (and especially the CRA) to determine what level of **Testing Rigor** they need the Security Assessment to achieve. Some assessments might require very little verification of control compliance assertions, while others will require very rigorous verification. See Section 1.3.7.2.3 *Levels of Testing Rigor* for details.

To gain efficiencies and reduce re-work, the ACT framework enables (and <Organization> requires) the Assessment Team to use existing data and information from various security and risk information sources and then to supplement testing with manual or automated testing where sufficient pre-existing data is not available. Therefore, it is important to determine and document during planning which data sources (including RIS’s) will be used during the assessment and what type of additional testing and data collection must be performed by the Assessment Team.

Inputs and Outputs for this section are:

* Inputs
  + ACT Intake Form (responsible role: BO/ISSO)
* Outputs
  + Assessment Test Plan (select 1 or 2) (responsible role: Security Assessment Lead or Risk Assessment Lead)
    - ACT Risk Assessment Plan
    - ACT Security Assessment Plan

### Start Assessment

The assessment process may start based on a variety of events depending on the application life cycle. Some common reasons for a Security Assessment are the Annual Assessment (sometimes called “annual 1/3”), Re-Authorization, a Major System Change triggered by a Security Impact Analysis, or the first time “Initial” Authorization for new systems. Common reasons for a Risk Assessment are the execution of a Security Assessment, the execution of some other type of assessment, or a late-breaking technical or procedural concern that requires risk analysis. Regardless of the reasons, the assessment starts with a request to the ACT Mailbox and contact with the CRA. Once this request is complete, the Security Assessment Lead or Risk Assessment Lead will provide the ACT Preliminary Intake Form Template (see Section 3 *Attachments*) to the BO/ISSO/ISSM in preparation for the Preliminary Discussion.

#### Create Assessment Folder on <Storage Location>

Immediately upon being informed that an assessment of a system is required, the Assessment Lead or Risk Assessment Lead (as appropriate) creates the folder structure on the <Organization>-provided <ACT data storage location> site that will be used to store the various assessment artifacts (both those received from the system team, and those created by the Assessment Team). The folder structure should be the same as the structure used for the Final Package (see Section 2.3.5.1 *Organization of Final Package* for details), and may additionally contain a private folder named “*00 NOT FOR FINAL PACKAGE - Internal Working Docs*” that will not be included in the Final Package.

#### Receive Preliminary Intake Form and Tier 1 Artifacts

Prior to the Preliminary Discussion, the Security Assessment Lead and the CRA will review the ACT assessment schedule for ACT Assessment Team availability. The Security Assessment Lead will send an email calendar invitation to the ISSO, GTL and CRA to schedule the Preliminary Discussion, along with a request for the Tier 1 artifacts (listed in the *Preliminary Intake Form* template) to be provided via <Organization’s Secure File Transfer System>.

The Security Assessment Lead receives the Tier 1 artifacts from the system team **no less than one (1) week prior to the Preliminary Discussion**, confirms receipt, and uploads them to the appropriate folder on the <Organization> <ACT data storage location>; if not received within this timeframe, the Security Assessment Lead shall raise the issue to all involved parties, including the ACT GTL, system CRA, and system ISSO. The Security Assessment Lead reviews the Preliminary Intake Form and Tier 1 artifacts for completeness and accuracy.

The Security Assessment Lead prepares for the Preliminary Discussion, populating the appropriate ACT Security and/or Risk Assessment Plan Template (see Section 3 *Attachments*). The Security Assessment Lead will potentially delay the preliminary meeting depending on quality and presence of Tier 1 artifacts and Preliminary Intake form.

### Conduct Preliminary Discussion

The purpose of the preliminary discussion is to review the assessment process, inform all involved parties of what to expect, and to collect all information required to produce the Assessment Plan. This call is held with the Security Assessment Lead and/or Risk Assessment Lead, CRA, the system ISSO, system stakeholders, and system contractors. The ACT Contractor arranges the meeting and sends email invitations to all parties involved. The Security Assessment Lead or Risk Assessment Lead prepares the ACT Preliminary Discussion Meeting Presentation utilizing the respective Template (see Section 3 *Attachments*). The meeting covers the following:

* Assessment methodology
* Validation of information to be used in the ACT Assessment Plan, taken from the ACT Intake form
* Review of test environment and testing to be conducted (for Security Assessments), assessment scope, and system boundaries
* Discussion about and determination of required level of Testing Rigor
  + If Level 3 is chosen, work with the CRA to determine what type of test sampling of the Non-Core Controls’ assertions will be acceptable. For example, the CRA might require that a certain random percentage of the Non-Core Controls’ assertions will be fully verified, or that all assertions for a specific set of Non-Core Controls will be verified, *etc.*
* Review assessment milestone dates
* Coordinate testing logistics (for Security Assessments)
* Coordinate on-site assessment logistics (if required)
* Discuss any user accounts that may be required (for Security Assessments, depending on the Level of Testing Rigor)
* Artifact transportation, encryption
  + A password to encrypt sensitive documents throughout the assessment is also established and documented in the Meeting Notes. Using a program (*e.g.*, SecureZip), documentation can be encrypted with a sufficiently complex password and 256-bit AES (or better) encryption.

The expected outcomes of the Preliminary Discussion are:

* Meeting Notes created by the Security Assessment Lead or Risk Assessment Lead or other designated person using the Meeting Notes Template (see Section 3 *Attachments*) and then distributed to everyone in the meeting. It is important to take roll and to have the correct names and email addresses of attendees when commencing the call.
* All information required for production of the Assessment Plan is provided before, at, or soon-after the Preliminary Discussion, prior to the Assessment Lead or Risk Assessment Lead writing the Assessment Plan. If the required information is not provided in a timely manner then it is likely that the Assessment Lead or Risk Assessment Lead will not be able to produce an adequate Assessment Plan, and the assessment schedule might need to be delayed.
* Document any action items that need follow-up for future pre-assessment period meetings.
* Follow up requests for missing Tier 1 artifacts if not already provided.
* Identify the assessment period testing timeframe and location (for Security Assessments)
* Agreement of the assessment’s authorization boundary and scope
* Discuss technologies deployed in the environment to be assessed

Typical actions following the Preliminary Discussion, if applicable:

* The Security Assessment Lead or Risk Assessment Lead provides:
  + Meeting Notes tracking the action items from the meeting
  + ACT Assessment Plan, based off information gained from the Preliminary Discussion and review of Tier 1 and Tier 2 artifacts
  + Scripts, scans, or technical data call items for the government vendors/contractors to provide prior to the assessment period (for Security Assessments). Examples of data call items include:
    - Operating system configurations
    - Network appliance configurations
    - Database configurations
    - Mainframe configurations, sample batch jobs, etc.
  + Finalized milestone schedule
* The ISSO, typically with assistance from application owners-contractors, provides:
  + Outstanding Tier 1 artifacts
  + Scripts, scans, and technical data call replies (for Security Assessments)
  + The provisioning of Assessor test accounts, with username/password (for Security Assessments)
  + Confirmation and access to testing environment with test data, if applicable (for Security Assessments)

Inputs and Outputs for this section are:

* Inputs
  + ACT Intake Form (responsible role: BO/ISSO)
  + ACT Preliminary Discussion Meeting Presentation (responsible role: Security Assessment Lead or Risk Assessment Lead)
* Outputs
  + Preliminary Discussion Conference Call Meeting Notes (responsible role: Security Assessment Lead or Risk Assessment Lead)

### Review Tier 1 Artifacts

The Security Assessment Lead or Risk Assessment Lead analyzes the system documentation received to determine the resources required to conduct testing, as well as aid in developing the ACT Assessment Plan. Documentation reviews can start as soon as the documents are available. For both Security Assessments and Risk Assessments, an initial review of the System Security Plan (SSP), Information System Risk Assessment (ISRA), Contingency Plan (CP), and Privacy Impact Analysis (PIA) documents and the Meeting Notes from the preliminary discussion meeting is necessary to understand the technologies deployed in the environment and the resources necessary to perform the assessment.

The expected outcomes of reviewing the Tier 1 artifacts are:

* A thorough understanding of the system’s authorization boundary
* An understanding of the resources required to conduct the assessment

Typical actions following the review of Tier 1 artifacts are:

* Development of the Security Assessment Plan and/or Risk Assessment Plan

Inputs and Outputs for reviewing Tier 1 artifacts are:

* Inputs
  + Tier 1 artifacts (responsible role: ISSO)
* Outputs
  + Notes for aiding in the development of the Assessment Plan (responsible role: Security Assessment Lead or Risk Assessment Lead)

### Develop Assessment Plan

The Security Assessment Lead or Risk Assessment Lead develops the Risk Assessment Plan or Security Assessment Plan for the system using either the *ACT Risk Assessment Plan template or the ACT Security Assessment Plan Template.* A sample Security Assessment Plan and a sample Risk Assessment Plan are provided in Section 3 *Attachments*, demonstrating best practices for producing these documents.

All the information required to complete the Assessment Plan should be found in documentation received from <Organization> (*e.g.*, SSP, ISRA, CP) as well as information gathered from the Preliminary Discussion Meeting. It is possible that additional questions will surface during the development of the Assessment Plan; these questions should be noted as comments in the document and then be discussed during the Assessment Plan Review Meeting. However, the Assessment Lead or Risk Assessment Lead should collect the vast majority of information required for production of the Assessment Plan *prior* towriting the Assessment Plan. If the required information is not received in a timely manner, then it is likely that the Security Assessment Lead or Risk Assessment Lead will not be able to produce an adequate Assessment Plan. **The Assessment Plan that is submitted for review at the Assessment Plan Review Meeting must be essentially complete and ready for formal publication and use, with only minor areas of concern to be addressed or minor questions still to be answered highlighted in the document.**

The expected outcomes of developing the Assessment Plan are:

* Understanding and documenting <Organization> requirements for the system’s assessment type
* Defining the assessment scope
* Defining any assumptions or limitations for the assessment
* Defining the ACT team required to adequately assess the system
* Defining all Points of Contact (POCs) for the ACT Team, <Organization>, and System Contractor personnel for the system

Typical actions following the development of the Assessment Plan are:

* Confirming ACT team staffing schedules for the assessment
* Scheduling the Assessment Plan Review Meeting

Inputs and Outputs for developing the Assessment Plan are:

* Inputs
  + ACT Assessment Plan (responsible role: Security Assessment Lead or Risk Assessment Lead)
  + Information from documents/artifacts review (responsible role: Security Assessment Lead or Risk Assessment Lead)
  + Preliminary Discussion Conference Call Meeting Notes (responsible role: Security Assessment Lead or Risk Assessment Lead)
* Outputs
  + Develop and deliver the ACT Assessment Plan (responsible role: Security Assessment Lead or Risk Assessment Lead)

#### Authorization Boundary and Assessment Boundary

It is critically important for the entire Assessment Team to understand the difference between the Authorization Boundary and the Assessment Boundary, and to ensure that they are both clearly and unambiguously defined in the Assessment Plan. In short: the Authorization Boundary defines *the extent of the* *authorized* *system itself*, while the Assessment Boundary defines *which parts of the authorized system are being assessed as part of the current assessment.* These two boundaries are described in detail below.

##### Authorization Boundary

NIST[[21]](#footnote-22) defines the “Authorization Boundary”[[22]](#footnote-23) as:

*All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.[[23]](#footnote-24)*

The Authorization Boundary is defined and documented via diagram and text by (and provided to the Assessment Team by) the system. **If the Authorization Boundary diagram and definition are insufficient, the assessment team must work with the system team to update the Authorization Boundary to minimum requirements.** Per <Organization Information Security Group> requirements, Authorization Boundary diagrams must:

1. Clearly document the Authorization Boundary: all components (and their connections) that comprise the authorized system (*i.e.*, what the Authorizing Official (AO) grants an Authorization to Operate (ATO) for).
   * Clearly define the Authorization Boundary with a predominant border, defined in the legend, drawn around all included system components and services. The boundary might comprise a single shape or multiple separate shapes.
2. Clearly document *interconnections* with other authorized systems (*i.e.*, other Authorization Boundaries).
   * Identify any connections to other systems/networks/enclaves, including:
     + The name of the organization that owns the system/network/enclave, *as appropriate.*
     + The connection type (*e.g.*, wireless, dedicated point-to-point), *as appropriate*.
     + The organization type (*e.g.*, <Organization>, another Federal agency, contractor), *as appropriate*.
     + Data flows clearly marked as unidirectional or bi-directional.
     + Protocols, ports, etc. in use by the system should be depicted *as appropriate*.
   * Note that sometimes components are *notionally* within the authorization boundary of the system but are actually part of / provided by one or more separate authorized systems.
3. Be clearly legible in the provided format (*e.g.*, no “pixelization”).
4. Provide a last-updated date and legend.
5. Identify equipment/component inventory consistent with documented hardware and software inventories (including firewalls, Intrusion Detection or Prevention Systems (IDS/IPS), routers, switches, Internet Protocol (IP) addresses, encryption devices, etc.).
6. Identify all cybersecurity or cybersecurity-enabled products deployed within the authorization boundary.
7. Use formal names for all components, ensuring that names match system documentation (*i.e.*, functional specifications, configuration guides, SSP)

*Note that for complex systems, multiple diagrams might be required to provide the appropriate level of detail.*

An example Authorization Boundary diagram[[24]](#footnote-25) is shown below.

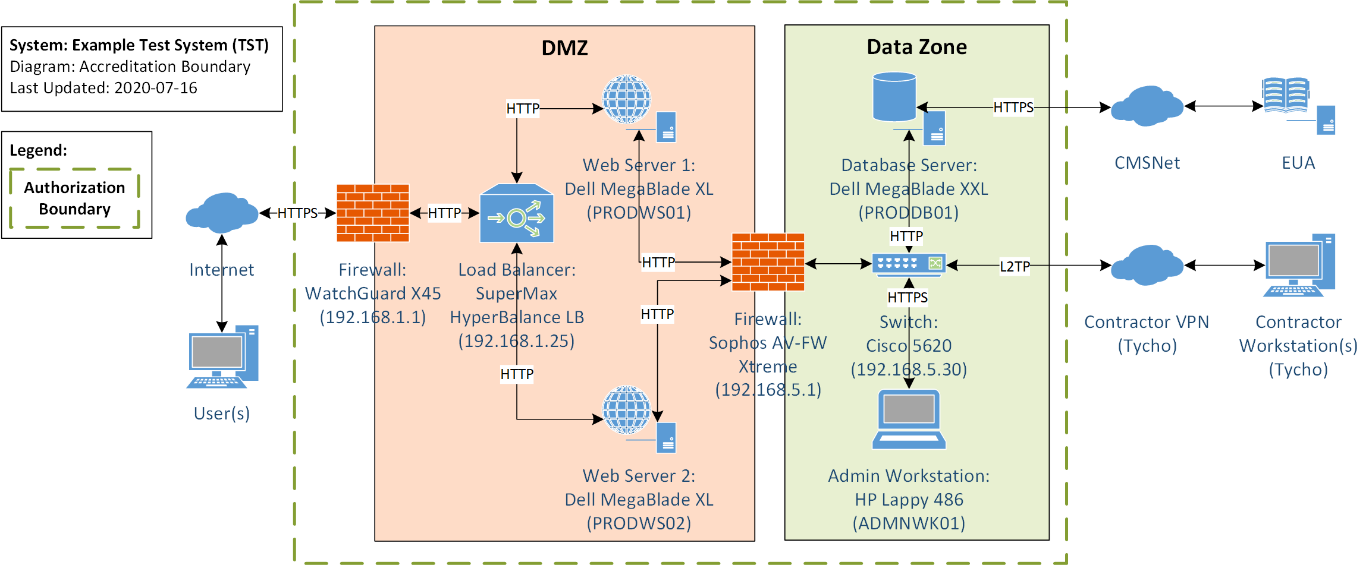


Figure 4. Example Authorization Boundary Diagram

##### Assessment Boundary

NIST defines the “Assessment Boundary” as:

*The scope of (assessment objects included in) an organization’s ISCM implementation to which assessment of objects is applied. Typically, assessment boundary includes an entire network to its outside perimeter.[[25]](#footnote-26)*

The Assessment Boundary is documented via diagram and text by the Assessment Team with the assistance of the system team. If possible, the Assessment Team should use the official (or updated) Authorization Boundary diagram/definition as the foundation of the Assessment Boundary. Per <Organization Information Security Group> requirements, Assessment Boundary diagrams must:

1. Be directly mappable to / understandable when compared to the Authorization Boundary.
2. Clearly document the Assessment Boundary: all components (and their connections) that are included in-scope for the current assessment (*i.e.*, which exact components, interfaces, etc. the Assessment Team will be testing, reviewing).
   * Clearly define the Assessment Boundary with a predominant border, defined in the legend, drawn around all included system components and services. The boundary might comprise a single shape or multiple separate shapes.
3. Be clearly legible in the provided format (*e.g.*, no “pixelization”).

*Note that for complex assessments or systems, multiple diagrams might be required to provide the appropriate level of detail.*

An example Assessment Boundary diagram[[26]](#footnote-27) is shown below.

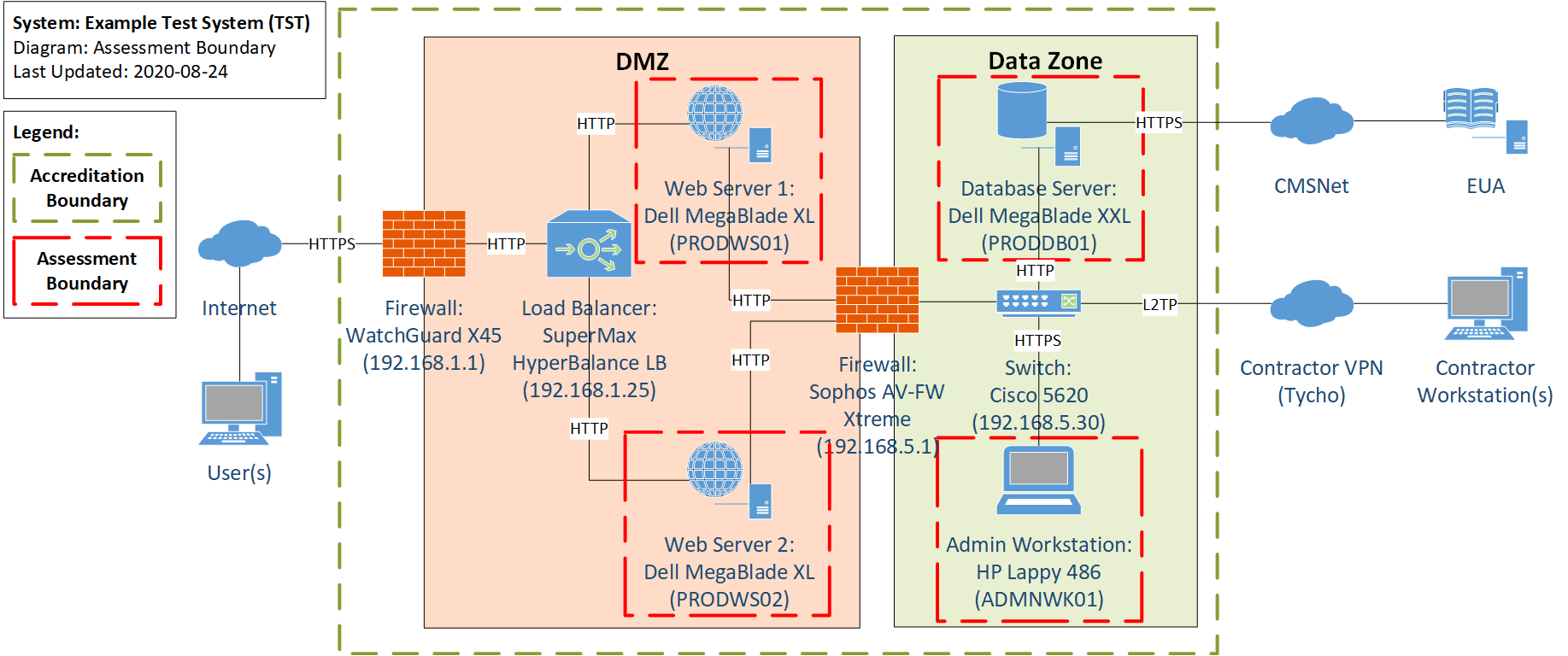


Figure 5. Example Assessment Boundary Diagram

### Conduct Assessment Plan Review Meeting

The purpose of the Assessment Plan Review is to confirm, and correct, if necessary, the information captured in the ACT Assessment Plan. The meeting is typically held at least four (4) weeks prior to the assessment period. The Security Assessment Lead or Risk Assessment Lead will update the Assessment Plan with any changes discussed during the meeting. This updated document will serve as the final Assessment Plan and shall be delivered after the Readiness Review Meeting and no later than one (1) business day before start of the assessment. Meeting Notes are created by the Security Assessment Lead or Risk Assessment Lead or designated resource and then distributed to everyone on the call.

The expected outcomes of conducting the Assessment Plan Review Meeting are:

* Confirmation of <Organization> requirements for the system’s assessment type
* Confirmation of the assessment scope
* Confirmation of any assumptions or limitations for the assessment
* Confirmation of all POCs for the ACT Team, <Organization>, and System Contractor personnel for the system

Typical actions following the Assessment Plan Review Meeting are:

* Ensure Tier 2 artifacts are requested
* Scheduling meeting invitations required for the assessment
* Compiling all Meeting Notes, notes, and actions for inclusion into the Final Assessment Plan

Inputs and Outputs for the Assessment Plan Review Meeting are:

* Inputs
  + Meeting Agenda, which can be verbal and does not require a soft or hardcopy (responsible role: CRA)
  + ACT Assessment Plan (responsible role: Security Assessment Lead or Risk Assessment Lead)
  + Meeting Notes from Preliminary Discussion Conference Call (responsible role: Security Assessment Lead or Risk Assessment Lead)
* Outputs
  + Meeting Notes with Action Items (responsible role: Security Assessment Lead or Risk Assessment Lead)
  + Meeting invitations for interviews and meetings (responsible role: Security Assessment Lead or Risk Assessment Lead):
    - Assessment Plan Review
    - Application demonstration (If <Organization> Apps are being assessed)
    - Readiness Review (Last meeting prior to assessment period)
    - Assessment Period interviews (multiple based on interview audience)
    - Daily Out briefs (typically at the end of each day of the assessment period)
    - Final Out brief (Last meeting of the assessment period)
    - Assessment Report Review

### Conduct Readiness Review Meeting

**For Security Assessments only**, the Readiness Review Meeting is scheduled (1) week before the assessment period. The purpose of this meeting is to ensure that all parties are ready for the assessment, that any remaining open action items have been addressed, such as missing artifacts, testing accounts or test data, and that any last-minute questions from the ACT Assessment Team or the government vendor/contractor are answered. The goal is to determine whether the environment is ready to test. This is the point where a Go/No-Go decision can be made prior to travel plans being executed. Meeting Notes are kept by the Security Assessment Lead or Risk Assessment Lead or designated resource and then distributed to everyone on the call.

The expected outcomes of conducting the Readiness Review Meeting are:

* Confirmation of system access and test accounts (local or remote, if required by Level of Testing Rigor)
* Confirmation that all system components within the authorization boundary are functioning and readily assessable
* A final Go/No-Go decision for conducting the assessment

Typical actions following the Readiness Review Meeting are:

* Follow up(s) for any last-minute questions by either the ACT Assessment Team or the government vendor/contractor

Inputs and Outputs for the Readiness Review Meeting are:

* Inputs
  + Readiness Review Presentation (responsible role: Security Assessment Lead)
  + ACT Assessment Plan (responsible role: Security Assessment Lead)
* Outputs
  + Meeting Notes with Action Items (responsible role: Security Assessment Lead)

### Assessment Team Preparation

**For Security Assessments only**, the assessment period preparations involve the completion of several additional tasks by various members of the ACT Assessment Team, <Organization>, and staff supporting the system being reviewed. Thorough preparations prior to the assessment period help ensure the success of the assessment period. These preparations/tasks include scheduling and holding an Internal Team meeting; scheduling assessment period interviews; ensuring that space at the government contractor facility has been reserved for the ACT Assessment Team; establishing and testing, if possible, the application accounts that will be used during the assessment; delivery of on-site network/application logon instructions; and contacting technical writer support with key dates for the report. Some tasks are internal to the ACT Assessment Team and may be handled differently depending on the Security Assessment Lead or Risk Assessment Lead. Since the step includes several distinct tasks, the details associated with this step are covered in this section.

The expected outcomes of the Assessment Team Assessment Period Preparation are:

* Confirmation of access and reserved space at the government contractor facility
* Confirmation that all required <Organization> and contractor personnel interviews have been scheduled and accepted

Typical actions following the Assessment Team Assessment Period Preparation are:

* Follow up(s) for:
  + Any outstanding ACT Assessment Team scheduling conflicts
  + Confirmation of access and reserved space at the government contractor facility

Inputs and Outputs for the Assessment Team Assessment Period Preparation are:

* Inputs
  + Assessment Plan (responsible role: Security Assessment Lead or Risk Assessment Lead)
  + All Notes from previous discussions and meetings (responsible role: Security Assessment Lead or Risk Assessment Lead)
  + Request for Test Accounts (responsible role: Security Assessment Lead or Risk Assessment Lead)
* Outputs
  + Assessment Test Account Provisioning (responsible role: CRA)

#### Assemble Assessment Team

From the information gathered during the application testing conference call step, the Security Assessment Lead or Risk Assessment Lead coordinates the technical, as well as management and operational, resources to build the ACT Assessment Team.

There are no expected outcomes or typical actions following the assembly of the Assessment Team.

The Inputs and Outputs for Assembling the Assessment Team are:

* Inputs
  + Assessment Plan (responsible role: Security Assessment Lead or Risk Assessment Lead)
  + Assessment Plan Review Meeting Notes with Action Items (responsible role: Security Assessment Lead or Risk Assessment Lead)
  + Application Testing Conference Call Meeting Notes with Action Items (responsible role: Security Assessment Lead or Risk Assessment Lead)
* Outputs
  + ACT Assessment Team (responsible role: Security Assessment Lead or Risk Assessment Lead)

#### Schedule and Conduct Internal Assessment Team Meeting

Two weeks or more prior to the assessment period scheduled date, convene an internal meeting with ACT Assessment Team members. Following the Internal Team Kick-off Meeting Template as guidance, including:

* Discuss the environment and security categorization (*i.e.*, High, Moderate, or Low)
* Assign roles and responsibilities
* Coordinate travel logistics
* Discuss reporting vulnerabilities (*i.e.*, <Organization> finding spreadsheet, correlation to <Organization Controls Catalog>, and <Organization> Minimum Security Configuration Standards for Operating Systems review of risk-level ratings)
* Answer questions

The meeting provides an opportunity to discuss the assessment period with the Assessment ACT Assessment Team and to answer any questions the team may have.

#### Schedule Assessment Phase Meetings

Contact the assessment period POC from either <Organization> and/or the government development contractor, (if external to <Organization>) to assist in scheduling interviews as outlined in the ACT Final Assessment Plan. While interview times can be subject to change, having an interview schedule determined before the assessment causes less confusion during the assessment period. Attempt to schedule the technical interviews midweek to provide the testers an opportunity to understand the system prior to conducting the interviews. The management and operational control interviews are typically scheduled Monday through Thursday of the assessment period week; the SSP, ISRA, CP, and PIA documentation reviews are typically scheduled on Thursday.

#### Reserve Meeting Rooms and Assessment Space (if necessary)

If the assessment is taking place onsite (for example, at the <Organization Data Center> or at a contractor facility), make arrangements with the CRA and/or ISSO/ISSM to reserve access to a workroom. This room can serve as both a testing and interview room.

#### Verify Application Test Accounts

The <Organization> accounts required for application testing, if necessary, should be identified. The Enterprise User Administration (EUA) job codes are assigned and supplied to the CRA. The CRA then completes the <Organization> USERID form *Application for Access to <Organization> Computer Systems,* for the test accounts to be authorized.

Ensure that all requirements are completed at least two weeks prior to assessment period to establish the test accounts needed to perform the technical application test, which requires coordinating with the CRA or business owner. If possible, after receiving the accounts and passwords, arrange access to the application and test the accounts to determine if they are established correctly and that the tester can successfully login with the account.

### Notify Technical Writer/Editor of Key Dates for Report

For both Security Assessments and Risk Assessments, provide technical writers with the deliverables schedule, including dates for at least the following:

* Assessment Report to Technical Writer
* Assessment Report to <Organization>
* Updated Assessment Report (with edits from the Assessment Report Review Call) to <Organization>

### Deliver Updated Assessment Plan

For both Security Assessments and Risk Assessments, the ACT Final Assessment Plan must have all outstanding items from the Assessment Plan Review Meeting addressed, along with the team composition and POCs completed. The updated Assessment Plan shall be delivered no later than (1) business day before the start of the assessment.

The expected outcome of delivering the updated Assessment Plan is:

* All outstanding items during Phase 1: Planning have been addressed and Phase 2: Assessment is ready to begin.

Typical actions following the delivery of the updated Assessment Plan are:

* Conduct Phase 2: Assessment

The Inputs and Outputs for Delivering the updated Assessment Plan are:

* Inputs
  + Assessment Plan (responsible role: Security Assessment Lead or Risk Assessment Lead)
  + Assessment Plan Review Meeting Notes with Action Items (responsible role: Security Assessment Lead or Risk Assessment Lead)
  + Application Testing Conference Call Meeting Notes with Action Items (responsible role: Security Assessment Lead or Risk Assessment Lead)
* Outputs
  + Updated Security Assessment Plan or Risk Assessment Plan (responsible role: Security Assessment Lead or Risk Assessment Lead)

## Phase 2: Assessment

The **Assessment** phase is typically one (1) week but can be longer, depending on the assessment type, security categorization, or complexity of the system. Technical testing should follow specific guidance based on the technology used and the controls to be assessed for a consistent and repeatable testing experience. The managerial and operational control testing is based on the security controls in scope for the assessment. All potential High-risk and Critical-risk findings are immediately discussed with <Organization> and the personnel responsible for the control implementation, any clarifications or additional information should be provided, and remediation efforts and plans should be discussed immediately.

For a **Risk Assessment**, this phase involves reviewing data from all available RIS and documenting resultant Risks; for a **Security Assessment**, this also involves technical testing of the system, review of system documentation, and conducting interviews.

The Security Assessment Lead or Risk Assessment Lead plays a crucial role in tracking outputs, requesting documents, handling problems with infrastructure access, and processing the technical test and closure evidence. Each Assessor documents potential findings in the Assessment Findings Template and provides them to the Security Assessment Lead or Risk Assessment Lead for consolidation and sorting by risk prior to the daily on-site out brief.

The following diagrams show the high-level flow of this phase for a Security Assessment in Figure 6 and for a Risk Assessment in Figure 7.

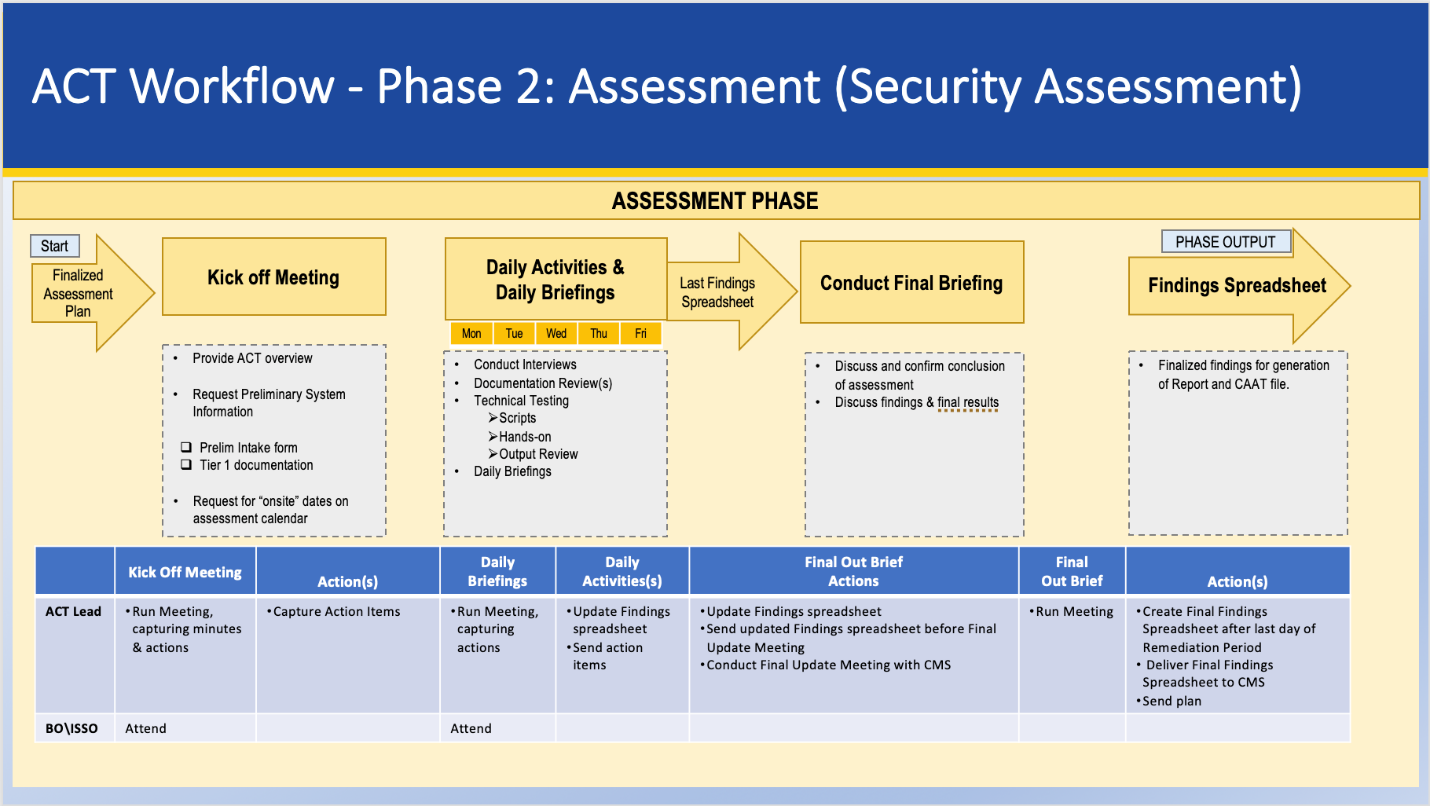


Figure . Phase 2: Assessment (Security Assessment)

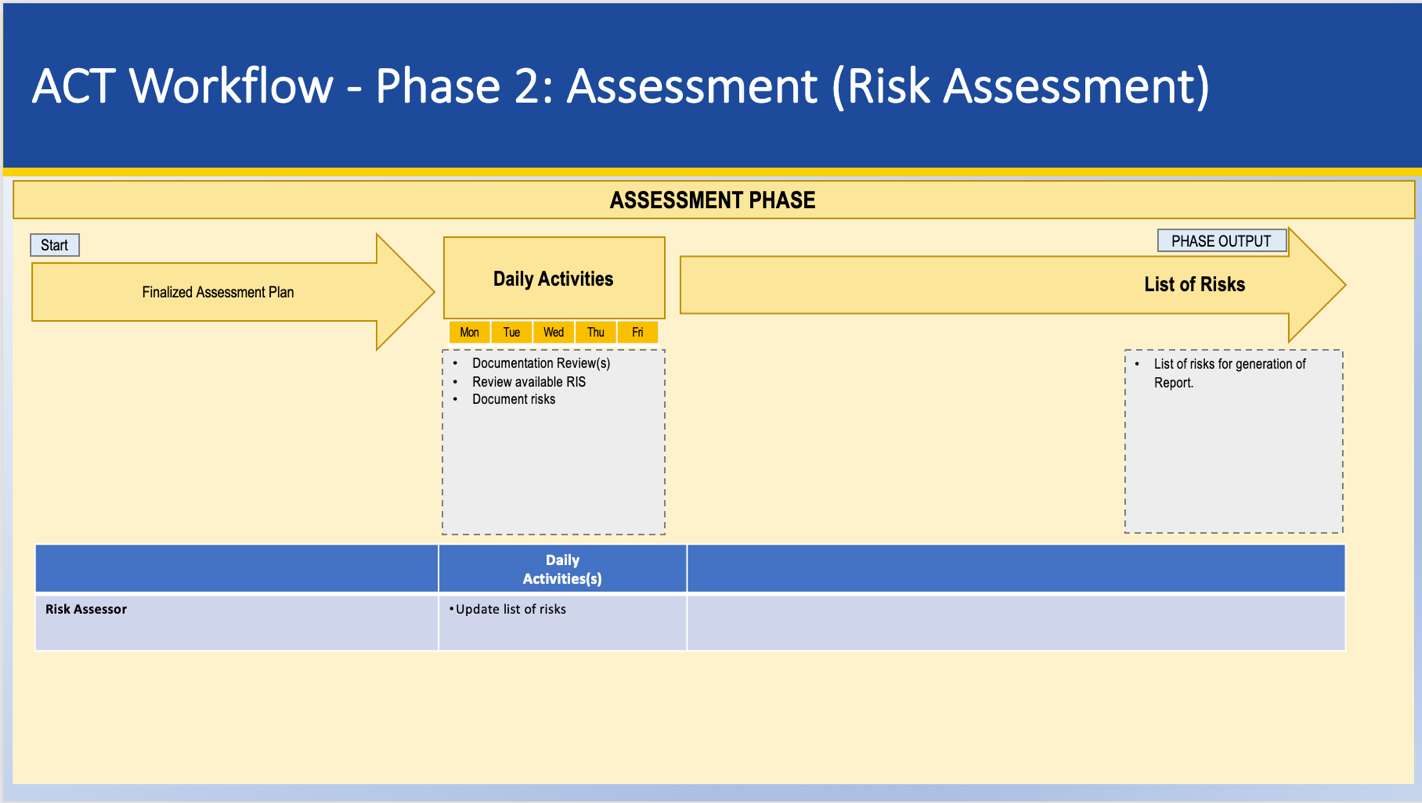


Figure . Phase 2: Assessment (Risk Assessment)

Inputs and Outputs for this section are:

* Inputs
  + ACT Assessment Kick-Off Meeting Presentation (responsible role: Security Assessment Lead or Risk Assessment Lead)
  + Assessment Findings Template (responsible role: Security Assessment Lead or Risk Assessment Lead)
* Outputs
  + A consolidated Assessment Findings Spreadsheet (responsible role: Security Assessment Lead or Risk Assessment Lead)

The following ACT Assessment Team members perform roles either on-site or remotely. The responsibilities of each role are described below.

### Security Assessment Lead

Security Assessment: This role is required.

The Security Assessment Lead is responsible for the overall success of the Assessment and therefore will spend the Assessment Phase monitoring and supporting the other Assessors and performing administrative tasks while the Assessors focus on technical assessment.

#### Conduct Security Assessment Kick-Off Meeting

The Security Assessment begins with the “kick-off” meeting which provides an opportunity to remind all participants of the assessment’s scope, review the schedule for interviews and out-briefs, to introduce the assessment Team, and to address any last-minute open action items.

The Security Assessment Lead should fill-in and follow the Assessment Kick-Off Meeting Presentation Template (see Section 3 *Attachments*)**.**

#### Coordinate All Activities

The Security Assessment Lead’s primary role during the security assessment period is to serve as the “glue” that joins all the different security assessment activities into a cohesive whole. The Security Assessment Lead monitors and works with each Assessor to understand and facilitate their testing; and to ensure that issues identified during testing are valid and are communicated to, understood, and considered by the other Assessors. The Security Assessment Lead also acts as the primary point of contact with <Organization> and any system contractors, providing a coherent and single voice for the Assessment Team. While the individual Assessors are responsible for successful execution of their portions of the assessment activities, the Security Assessment Lead is ultimately responsible for the successful and complete execution of the entire assessment.

#### Ensure Storage of All Artifacts in <Storage Location>

Throughout the entire process, the Security Assessment Lead ensures that all assessment artifacts – both those received from the system team and those created by the Assessment Team – are uploaded to the appropriate folder on the <Storage Location> in a timely manner.

#### Consolidate, Review, Edit, and Publish Findings

As Findings are reported to the Security Assessment Lead by the individual Assessors, the Security Assessment Lead consolidates, reviews, corrects, and de-duplicates or combines them (if appropriate), feeding these changes back to the individual Assessors and publishing them to the system stakeholders. The Security Assessment Lead also ensures that each Finding is assigned Impact and Likelihood levels, and the overall Risk level is calculated from those two values, using the methodology specified in Section 1.3.8 *Risk Scoring Methodology*.

#### Attend and Support All Meetings

The Security Assessment Lead attends and supports all assessment meetings and interviews to maintain awareness and control of the assessment and to ensure that all necessary actions are taken and that the appropriate information is presented in the appropriate manner.

#### Hold Daily Briefings

After the first day of the assessment period, daily out-briefs are conducted to review and vet any potential findings. The assessment findings are combined from all Assessors and sorted by risk level (Critical, High, Moderate, and Low) or Common Vulnerability Scoring System (CVSS) score on the Assessment Findings Spreadsheet Template (see Section 3 *Attachments*). Prior to the outbrief, the Security Assessment Lead reviews the findings for content, quality, appropriate risk level, and accurate recommendations. If there are questions regarding a specific finding, the Security Assessment Lead consults the Assessor and, if needed, seeks clarification on the issue from the GTL or the government vendor/contractor.

The Security Assessment Lead prepares the daily briefing agenda utilizing the Daily Briefing Agenda Template to document outstanding items and issues (see Section 3 *Attachments*). If necessary, open action items from previous Meeting Notes are placed in the agenda. The agenda indicates the testing areas that need to be completed for the remainder of the week. Once both the consolidated findings and the daily out-brief agenda are complete, the Security Assessment Lead or Risk Assessment Lead sends them to the CRA and all system stakeholders via an encrypted zip file. During the out-brief, the discussions focus on Critical, High, and Moderate risk-level findings; however, if time allows or if desired, Low risk-level findings are also discussed.

Inputs and Outputs for this section are:

* Inputs
  + Daily Briefing Agenda (responsible role: Security Assessment Lead)
  + Assessment Findings Spreadsheet (responsible role: Security Assessment Lead)
* Outputs
  + ACT Daily Briefing Agenda Updated Status of Action Items (responsible role: Security Assessment Lead)
  + Updated Consolidated Assessment Findings Spreadsheet (responsible role: Security Assessment Lead)

#### Finding Remediation During Assessment Period

During the assessment period (as defined in the Assessment Plan), findings may be remediated by the system’s staff if the Assessors have completed testing and/or agree that the remediations may be implemented while testing continues. If time allows and at the Lead’s discretion, additional testing may be conducted to verify that the finding has been closed. If this is the case, the findings spreadsheet should be updated with additional information about the remediation and denote the finding status as ‘closed’; the finding should not be removed from the spreadsheet (or the subsequent Report), which would make it appear that the finding never existed.

#### Remediation Period (Optional)

By default, ACT Security Assessments do not contain a remediation period. A “remediation period” is an *optional* period of time *after* the assessment period (defined in the Assessment Plan) and *before* the Report is written, during which time the system team may remediate findings and the assessment team may re-test and verify closure of those findings. Unless the CRA and GTL explicitly authorize a remediation period for a specific ACT Security Assessment, all remediation and re-testing must occur during the assessment period. If a remediation period is authorized, the length of time will be specified by the CRA or GTL.

#### Conduct Final Briefing (and Optional Remediation Review)

If the Assessment Team requires additional time after the last Daily Briefing to complete their review or test activities, the Lead may schedule a Final Briefing for the week following the assessment period. Note that all review and testing activities should be completed during the assessment period defined in the Assessment Plan unless otherwise agreed by the CRA (*i.e.*, the review and test activities should not extend into the following week without explicit agreement from the CRA). If additional findings are generated from this review, the Lead sends out an updated findings spreadsheet prior to the Final Briefing. The Security Assessment Lead and team members, together with the CRA, Business Owner, ISSO, and Government vendor/contractor may close findings during the ACT engagement. During the assessment period (and potentially during the optional remediation period), closure and mitigating evidence may be provided to the Security Assessment Lead. Findings that are addressed will reflect a closed status in the Security Assessment Report, while the remaining findings will reflect an open status.

Inputs and Outputs for this section are:

* Inputs
  + Daily Briefing Agenda (responsible role: Security Assessment Lead)
  + Possible Closure Evidence (responsible role: government vendor/contractor)
  + Consolidated Assessment Findings Spreadsheet (responsible role: Security Assessment Lead)
* Outputs
  + ACT Daily Briefing Agenda Updated Status of Action Items (responsible role: Security Assessment Lead)
  + Updated Consolidated Assessment Findings Spreadsheet (responsible role: Security Assessment Lead)

### Risk Assessment Lead

Risk Assessment: This role is mandatory.

While the other Assessor roles perform technical testing and generate risk information, the Risk Assessment Lead focuses exclusively on analyzing existing Risk Information Sources (RIS) (regardless of generation source). Put another way, the other Assessor roles generate a RIS that is (potentially) used by the Risk Assessment Lead (possibly along with other RIS) to determine the risk posture of the system being assessed. The Risk Assessment Lead role is utilized whenever a Risk Assessment Report (RAR) is requested, and the Risk Assessment Lead integrates with the Assessment Team when a RAR is requested along with a SAR.

The Risk Assessment Lead typically works independently of and after the other Assessors. The Risk Assessment Lead is not typically a part of the Security Assessment team but works closely with the Security Assessment team members and works closely with any Risk Assessors (see Section 2.2.3) assigned to the Risk Assessment.

#### Coordinate All Activities

The Risk Assessment Lead’s primary role during the risk assessment period is to serve as the “glue” that joins all the different risk assessment activities into a cohesive whole. The Risk Assessment Lead monitors and works with each Risk Assessor to understand and facilitate their analysis; and to ensure that issues identified during analysis are valid and are communicated to, understood, and considered by the other Risk Assessors. The Risk Assessment Lead also acts as the primary point of contact with <Organization> and any system contractors, providing a coherent and single voice for the Assessment Team. The Security Assessment Lead is ultimately responsible for the successful and complete execution of the entire assessment.

#### Ensure Storage of All Artifacts in <Storage Location>

Throughout the entire process, the Risk Assessment Lead ensures that all assessment artifacts – both those received from the system team and those created by the Assessment Team – are uploaded to the appropriate folder on the <Storage Location> in a timely manner.

#### Review System Documentation

Before identifying the risks to the system, the Risk Assessment Lead first familiarizes herself with the system by reviewing the system’s SSP, ISRA, PIA, and any existing ACT RARs. The purpose of this review is to understand the purpose, design, implementation, and environment of the system; its development roadmap; and the already-identified risks to the security and privacy of the system.

#### Review All Available Risk Information Sources Data

The Risk Assessment Lead reviews and analyzes the data from all available RIS (including the Findings and output from ongoing ACT Security Assessments). Available RIS might include ACT Security Assessments that are being conducted concurrently or that were conducted in the past; other available RIS might include sources such as penetration testing performed by the <Organization’s SOC/NOC>, DHS Cyber Hygiene, etc. The Risk Assessment Lead works with <Organization Information Security Group> and/or the appropriate Security Assessment Lead to determine which Risk Information Sources should be considered for each Assessment. The Risk Assessment Lead is responsible for ensuring that the data in the various in-scope RIS are valid and useful – if RIS data appears to be wrong, out-of-date, or otherwise not useful for Risk Assessment purposes, they should raise this issue to the CRA and GTL for guidance.

#### Document Risks

The Risk Assessment Lead uses the ACT Risk Identification Workbook to identify Risks, then documents them in the current version of the ACT Risk Assessment Report Template (Section 3 *Attachments*). The Risk Assessment Lead also ensures that each Risk is assigned Impact and Likelihood levels, and the overall Risk level is calculated from those two values, using the methodology specified in Section 1.3.8 *Risk Scoring Methodology*.

### Risk Assessor

Risk Assessment: This role is optional.

The Risk Assessor is an optional role that is utilized when the Risk Assessment Lead requires additional support. The Risk Assessor supports the Risk Assessment Lead by assisting with all aspects of the Risk Assessment as directed by the Risk Assessment Lead.

### Management and Operations (M&O) Assessor

Security Assessment: This role is required when significant documentation review is required.

Summary of M&O Assessor responsibilities:

* Determine whether the operational, managerial, and technical controls of the systems are implemented correctly to protect the CIA of the information processed by those systems in accordance with <Organization> policies and procedures.
* Assess the consistency between the system documentation (including all relevant supporting documentation) and the system implementation.
  + Note that documentation might not take the form of traditional self-contained MS Word or .pdf documents; many systems store relevant information in systems like Confluence, wikis, etc.
* Develop Security Documentation Evaluations using the <Organization>-provided Evaluation Templates. Attachment 5 includes the security documentation evaluation templates, one for each of the Information Security Risk Assessment, System Security Plan, and Contingency Plan. If the Contractor prefers to provide this information in another format, these documents must be approved by the Contract GTL(s) in advance for each instance. Each of the following Security Documents received prior to each ACT must be evaluated using the <Organization>-provided Evaluation Templates, the evaluations provided during the assessment period, and also included in the working papers:
  + System Security Plan
  + Information Security Risk Assessment
  + Contingency Plan and associated documents (*e.g.*, Tabletop Test and After-Action Report)
  + Privacy Impact Assessment (if no separate Privacy Assessor)

The M&O Assessor is responsible for performing an analysis of the various system artifacts, policies, procedures, and processes to identify deficiencies. Responsibilities include: attaining an accurate understanding of the system architecture; reviewing core ACT system artifacts, such as the SSP, ISRA, POA&M, and PIA; identifying deviations from best security practices; recording findings and consulting with other Assessors and the assessment lead to verify/corroborate findings; writing findings for the daily briefing; interviewing system staff, such as the BO, ISSO, and Cyber Risk Advisor (CRA); and presenting M&O findings during the daily stakeholder briefing.

This section is intended to serve as practical guidance for individuals conducting M&O related responsibilities for <Organization> ACT assessments. This section focuses on testing and evaluation techniques for M&O controls that <Organization> requires to be in place for infrastructures, systems, and applications in support of <Organization> business needs. Management controls involve those safeguards and countermeasures that manage information and information system security and the associated risks to <Organization> assets and operations. Operational controls support day-to-day procedures and mechanisms to protect <Organization> information and information systems.

Depending on the assessment’s scope, the M&O controls that need to be reviewed will change. The scope’s testing determination will be made during the initial Planning Phase between the BO, ISSO, and CRA.

During the planning phase, the M&O Assessor reviews the Adaptive Capabilities Testing (ACT) Assessment Plan to understand the assessment’s scope. Based on the scope, the <Organization> security policies, requirements and procedures are reviewed to ensure an understanding of those that are applicable to the current assessment. As system documentation is received, the M&O Assessor reviews the documentation to ensure he/she has full knowledge of the system to be assessed in coordination with the assessment’s scope. The M&O Assessor also determines any additional requests to ensure that the assessment period runs smoothly. During this time, any special testing requests are provided to the ACT Security Assessment Lead or Risk Assessment Lead so he/she can contact the system’s Point of Contact (POC) and any applicable <Organization> representatives (ex. CRA, Government Task Lead (GTL)) to ensure all requirements for the test are complete.

During the assessment phase, the M&O Assessor’s activities consist mainly of documentation review, ATO document evaluations, personnel interviews, facilities tour (if applicable) and overall analysis of implemented processes. The activities and the detailed supporting processes and procedures must be at an adequate level to determine compliance with controls at each applicable system impact level (Low/Moderate/High).

The M&O Assessor shall leverage the interview outlines provided in the following subsections and modify their testing procedures as needed. Table 8. M&O Assessor Checklist provides a mechanism for the Assessor to ensure completeness of his/her responsibilities with respect to the assessment’s scope.

Table . M&O Assessor Checklist

| **Task** | **Description** |
| --- | --- |
| Receive Documents | System Security Plan (SSP) |
| Information System Risk Assessment (ISRA) |
| Contingency Plan (CP) |
| Contingency Plan Table-Top Test Results |
| Contingency After Action Review (AAR) |
| Hardware/Software Inventories |
| Authorization Boundary Diagram |
| Data Flow Diagram |
| Privacy Impact Assessment (PIA) |
| Memoranda of Understanding (MOU)  Guidance: Any interconnection and/or information sharing between <Organization> systems needs a signed MOU. |
| Interconnection Sharing Agreements (ISA)  Guidance: Any interconnection and/or information sharing between a <Organization> system and an external (non-<Organization>) system needs a signed ISA. |
| Rules of Behavior |
| Review Documents | Review Documents to gain understanding of system. |
| Request/Track Documents | Request and track documents that may have been referenced in the SSP, ISRA, and CP for further understanding and clarity of Management and Operations. |
| Evaluate Documents | Evaluate the SSP using the System Security Plan Evaluation Template (see Section 3 *Attachments*) During this evaluation ensure that all requirements in the <Organization Controls Catalog> for each control are addressed (Have a copy open as the SSP detailed control information is evaluated). |
| Ensure that the URL domain names for production associated with public Web facing applications conform to OMB and <Organization/Division> policies for domain naming which states they must be ‘.gov’ websites:  Check with the technical Assessors to verify. |
| Evaluate Information System Risk Assessment (ISRA) using the Risk Assessment Evaluation Template (see Section 3 *Attachments*). Ensure the risk levels are set as required by the <Organization> guidance. |
| If the ISRA states that a risk acceptance has been granted, all CISO acceptance letters must be requested. Note that these letters are only valid for a year. If not provided, this is a finding. |
| Evaluate Contingency Plan (CP) using the Contingency Plan Evaluation Template (see Section 3 *Attachments*). Ensure the document addresses all requirements for recovery of the application specifically or by reference to another document. |
| Review PIA validating the following:   * The system requires a SORN[[27]](#footnote-28) if the following are true:   + Records are maintained by a Federal agency.   + The records contain information about an individual.   + The records are retrieved by a personal identifier. * Applications hosted in the Cloud, using cloud tools, the application may not necessarily need a <Organization> SORN. It may need a SORN from a different Agency. * Check the date of the PIA to ensure it is no more than one year old. |
| Provide Security Assessment Lead and the CRA with copy of the SSP, ISRA and CP evaluations. |
| Provide ISSO/ISSM and Business Owner with electronic copies of the SSP, ISRA and CP evaluations. |
| Review scope of the assessment, interview schedule and adjust or modify templates as needed. (Example: the ISSO/ISSM will be handling all CP questions. If so and depending on the schedule, you may want to cover those questions during the ISSO/ISSM interview). |
| Interviews | Conduct the following interviews, if applicable, using the relevant section of the Questionnaire-Management and Operations (see Section 3 *Attachments*):   * Awareness and Training * Application Developer * Information System Security Officer (ISSO) * Business Owner * Cyber Risk Advisor (CRA) * Configuration Manager * Contingency Planning * Human Resources / Personal Security * Incident Response Team/Manager * Program Manager   Record all responses as artifacts as required.  Notify Security Assessment Lead of any additional required interviews. |
| Facility Tour  (If applicable) | Complete the Facility Tour Checklist (see Section 3 *Attachments*) if in scope of the assessment. Record all notes and artifacts requested. |
| Attend Additional Interviews | Attend the other Interviews, if applicable.  Record all notes and artifacts requested. |
| Prepare List of Artifacts Requested | Provide list of artifacts to Security Assessment Lead as requested. |
| Review all Artifacts Received | Review all M&O and technical findings to determine if there are any broader M&O findings (*i.e.*, poor implementation of CM processes based on inconsistent configurations across components, broad problems with account management, etc.) |
| Prepare M&O Findings Daily | All non-electronic evidence or artifacts received and kept during the assessment must be scanned in and uploaded into the appropriate assessment folder (working papers, evidence, etc.) |
| Review All Findings | Review all findings as they are reported by the other Assessors. |
| Scan All Hardcopy Artifacts to Files | Add to repository for inclusion in Final Package. |
| Upload all Notes | Add to repository for inclusion in Final Package. |
| Upload all Electronic Artifacts | Add to repository for inclusion in Final Package. |

#### Physical Security / Facilities Tour

If the scope of the ACT assessment includes security capabilities and sub-capabilities which map to Physical and Environmental Protection Controls, a physical tour of the facility is conducted. The assessment of these controls is also based on observations that may begin as the M&O Assessor enters the building that houses the system(s) and/or data center. The facility assessment includes the data center, any supporting areas such as the areas housing telecommunications equipment, the support staff work environment, the exterior of the building, physical access control systems, internal and external monitoring equipment and supporting systems, and power and backup power equipment. During the tour, assessment of security capabilities and sub-capabilities which map to the Maintenance Controls and the Media Protection Controls are also completed. A Facilities tour check list can be found in Section 3 *Attachments*.

Technical Assessors may accompany the M&O Assessor to gain an understanding of the components that are being assessed.

Based on the procedures noted during the tour, the M&O Assessor requests and reviews additional supporting documentation.

#### Conduct Interviews

Documenting security controls does not ensure that the control is properly implemented. The M&O Assessors must ensure that the controls, as documented, are adequate and properly implemented. Technical Assessors are encouraged to assist the M&O Assessor to validate control implementation(s). The M&O Assessor and any technical Assessor(s) confirm through the interview process that the controls are implemented as stated, that the documentation is understood and followed, and that updates and changes are properly distributed to all support staff as needed.

Key information to confirm security controls are properly implemented is gained through personnel interviews. The M&O Assessor and any necessary technical Assessors interview the designated subject matter experts (SME) identified in the ACT Assessment Plan. These SMEs have specific knowledge of overall system security requirements as well as a detailed understanding of the information system’s operational functions. All staff with system responsibilities may be interviewed by the M&O Assessor depending on the assessment’s scope.

The interviews are based on individual roles and responsibilities, the organizational structure of the data center/facility hosting the system, and/or the ACT assessment’s scope. Although the initial identification of interviewees is determined during the ACT assessment’s Planning Phase, additional interviewees may be identified during the ACT assessment. The M&O Assessor is involved in interviews of technical support staff to ensure that M&O controls are followed as stated.

If personnel support multiple functions (*e.g.*, configuration management and contingency planning), the M&O Assessor may combine interview topics while meeting with the personnel. The interview questions focus not only on areas for which the interviewee may be directly responsible, but also include questions to validate that documented policies and procedures are understood, followed by support staff, and documented controls are implemented consistently across the organization. Although a policy or procedure may exist that implies a control is properly implemented, interviews with staff using the policy or procedure may reveal they are either not being consistently used or are being bypassed completely. An example of this would be if personnel have no knowledge of the procedure, thus it would be a finding.

The M&O questions are based on the <Organization> test objectives noted in the latest version of the <Organization> Acceptable Risk Safeguards (<Organization’s Controls Catalog>). During the background overview or in response to other questions, the interviewee may partially or completely cover the response to another question throughout this process. In that case, some questions may not be asked again; however, the M&O Assessor should ensure that the control was adequately addressed earlier. If necessary, the M&O Assessor could state “Although the implementation of this control may have been covered partially during an earlier response, I would like to review the implementation of the control again.” Additionally, some questions may not need to be asked based on the response to prior questions. Not all questions in the interview guidance need to be asked; they are for reference. The M&O Assessor is responsible for ensuring that all controls are covered, thus it is important to at least review each set of questions to ensure that the responses to the control implementation are adequately addressed.

Based on answers to the questions, additional information or artifacts should be requested to support the response(s). Possible artifacts or documentation to be requested is covered in the “Supporting Documentation/Evidence” section of the outlines. For example, if the SSP states that CM procedures are in place, the Assessor should request copies of these procedures and review them to ensure they satisfy requirements as outlined in the latest version of the <Organization’s Controls Catalog>. It is important that the document request be made. To thoroughly test a process, request related documents (*e.g.,* a specific CR reflecting a change and the corresponding audit reports or logs). Information on the CR and the individual responsible must be passed on to the ACT Security Assessment Lead or Risk Assessment Lead for follow-up.

#### Review Documentation

Complete documentation reviews (SSP, ISRA, CP, PIA).

The evaluation of documentation is a mandatory part of the assessment process which can be very time-consuming. Evaluation of the documents should take place as soon as possible, even prior to the formal start of the *Assessment* phase if possible, and pertinent information stated in the documents should be shared with the other Assessors and confirmed through technical testing. Review of the documents prior to the interviewing of stakeholders might obviate the need to ask certain questions during the *Assessment* phase.

##### Documentation Evaluations

Although all members of the ACT Assessment Team review the core security documents (SSP, ISRA, CP, and PIA) for various *specific* reasons, a *detailed and comprehensive* analysis of each document is prepared by the M&O Assessor. The accuracy and completeness of these documents is crucial for correctly describing the system’s potential security posture. Furthermore, these documents are required by policy for the SA&A package that is provided to the <Organization> Chief Information System Officer (CISO) for the Authorization to Operate (ATO). Their adequacy and completeness will be determined based on the appropriate <Organization> guidelines for each document. The detailed review evaluations will be provided to the system’s ISSO/ISSM and the business owner during the assessment period at a meeting that focuses on the documents’ evaluation results.

Inputs and Outputs for this section are:

* Inputs
  + Current SSP for system being assessed (responsible role: ISSO)
  + Current ISRA for system being assessed (responsible role: ISSO)
  + Current CP for system being assessed (responsible role: ISSO)
  + Current PIA for system being assessed (responsible role: ISSO)
* Outputs
  + System Security Plan Evaluation (responsible role: M&O Assessor)
  + ISRA Evaluation (responsible role: M&O Assessor)
  + Contingency Plan Evaluation (responsible role: M&O Assessor)

#### Consult with Other Assessors

The ACT Assessment Team performs as an integrated and cohesive team. Findings identified in respective assessment areas, such as Network, Operating System, Application, and Database, often overlap (*e.g.,* a weak web application I&A function may confirm weak or non-existent I&A processes/procedures/policies). These findings are shared within the team at least daily in preparation for the daily out-brief stakeholder meeting, but it is encouraged that findings and information are shared more often. This serves many purposes: to inform other Assessors, to confirm identified vulnerabilities are not false positives, and helps ensure the Assessors function as a team.

#### Document Findings

M&O findings focus on the deficiencies discovered in the security/privacy artifacts the M&O ACT team member is responsible for assessing as well as those elicited in interviews with system personnel. These include the SSP, CP, ISRA, POA&M, PIA, system inventories, and any system processes, procedures, and policies that are missing or need to be enhanced.

All findings in their respective assessment areas are documented by the ACT team to ensure tracking and eventual closure by the system staff. Findings are presented during the daily out-brief call and are typically confirmed with system personnel prior to the call. These findings are considered *draft* findings until confirmed.

If a High or Critical severity finding is discovered by the Assessment Team, the Security Assessment Lead or Risk Assessment Lead will immediately notify the CRA and arrange for a meeting with the appropriate stakeholders, typically the CRA, BO, and system personnel, responsible for the affected system component or process. If it is later determined that a finding is a false positive, it will remain as reported and documented as such.

#### Conduct Documentation Review Feedback Meeting

Once the M&O Assessor has completed the SSP, ISRA, CP, and PIA evaluations using the <Organization>-provided templates, the completed templates are sent to the Security Assessment Lead or Risk Assessment Lead for review and comments. The evaluations are then sent to the system stakeholders. A meeting is then convened to review the documentation evaluations with system stakeholders to answer any questions. Meeting participants may include the BO, ISSO, and CRA.

### Application Assessor

Security Assessment: This role is required when application testing is required.

Summary of Application Assessor responsibilities:

* Determine whether the assertions made in documentation and interviews are correct by exercising and testing the system’s functionality.
* As directed, focus on testing the application and database components of the system, with less focus on underlying operating systems, network devices, etc. unless otherwise determined during the planning phase.
* Follow the guidance provided by each Control’s “Assessment Methods and Objects” in the current version of the <Organization’s Controls Catalog>, industry best practices, and all other relevant <Organization> guidance and directives for all technical testing.
* Discover the design, implementation, and operational flaws that could violate <Organization> IS Policies, Standards, Procedures and Guidelines; Business Partners System Security Manual (BPSSM); and other standards (where applicable).
* Assess the susceptibility of the system to insider-, intranet-, Internet-, and network-based attacks.
* Review existing POA&Ms, as directed by <Organization>.
* Ensure adequate testing of every in-scope capability and sub-capability (and corresponding controls and control enhancements) in the <Organization’s Controls Catalog>.
* Verify all control inheritance assertions and document any issues with inheritance.
* Ensure that the technical testing portions of the ACT are performed in a non-production environment that is a near copy of the production environment. It is assumed that technical testing in production is best, but active technical testing in production may cause disruption, loss, or corruption of data or service. Technical testing may only be performed in a production environment with prior written approval from the system ISSO/ISSM or <Organization> Business Owner, the CRA, and the GTL.
* To the extent possible, the Assessor shall work with <Organization> and support contractors to use existing scan results from available tools. The Assessor shall review the scan configuration, ensure scans are credentialed where applicable, and ensure scans include all assets in scope.
* Use assessment tools that are acceptable to the GTL.

The Application Assessor is responsible for performing hands-on technical testing of the application. Responsibilities include: attaining an accurate understanding of the application logic and architecture; performing manual testing; using automated tools to scan and send data to the application to observe application behavior; performing an analysis of application behavior and examining automated tool output to identify vulnerabilities; identifying deviations from best application security practices; recording findings and consulting with other Assessors and the assessment lead to verify/corroborate findings; writing findings for the daily briefing; interviewing application system staff; and presenting application findings during the daily stakeholder briefing.

This section is intended to serve as practical guidance for individuals conducting the application evaluation for <Organization> ACT assessments. Specific attention will be given to application testing from a technical configuration perspective to assist the Application Assessor in determining the following: 1) whether application security controls have been implemented; 2) are working as intended; and 3) producing the desired results.

Guidance focuses on technical testing for web applications, web services, and thick-client applications. Testing the security of such systems requires experienced Assessors familiar with a multitude of application programming languages, technologies, components, and testing tools. It is assumed an Application Assessor will have considerable understanding and hands-on experience in these areas.

In many cases, performing an application security test has the potential to modify production data, system configurations, and system availability. Care should be taken to understand how certain tests impact the system. It is highly recommended to perform tests in a validation/test /pre-production environment where the application emulates the production instance, rather than testing the production application itself. However, efforts must be made to understand all environmental differences between the production and validation/test/pre-production environments and how these differences affect the test results.

#### Review Documentation, Script Output, and Configs

During the planning phase, the Application Assessor reviews the Assessment Plan to understand the scope of the assessment before reviewing the <Organization> security policies, procedures, and requirements. As system documentation, script output, and configurations are received, the Application Assessor reviews the information to ensure he/she has a full understanding of both the system being assessed, and the components being evaluated. To ensure an efficient application assessment, the Application Assessor confirms access to the application using assigned test accounts prior to commencement of the on-site assessment. The Application Assessor also determines any additional requests required to conduct the assessment. These requests are communicated with the ACT Security Assessment Lead or Risk Assessment Lead so that he/she can communicate with the system’s point of contact (POC) and any applicable <Organization> representatives (*e.g.* CRA, GTL).

#### Conduct Technical Testing

During the assessment phase, the Application Assessor’s primary responsibilities consist of tool selection, technical application testing, and personnel interviews. All activities, processes and procedures must be at an adequate level to determine compliance with controls at the applicable system impact level (Low/Moderate/High).

There are no technical-related Application Assessor evaluations for Awareness and Training (AT), Certification, Accreditation, and Security (CA), Contingency Planning (CP), Incident Response (IR), Maintenance (MA), Media Protection (MP), Physical and Environmental Protection (PE), Planning (PL), Personnel Security (PS), Risk Assessment (RA), System and Services Acquisition (SA), and Program Management (PM).

*A thorough, hands-on technical test of a typical application usually requires approximately 40 hours of testing by at least two (2) Application Assessors, no matter the testing scope – whether a comprehensive test or 1/3 of the security controls, due to the complexity of modern applications and varied technologies and components present in the authorization boundary.*

The following tables presents focus areas and some examples for technically evaluating applicable controls for a Moderate system, decomposed by area.

Table . Application Testing Focus Areas

|  |  |
| --- | --- |
| Application Test Focus Area | Description |
| Session Control | This area examines secure session establishment and termination; token replay; secure protocol use; and concurrent sessions. |
| Identification & Authentication | Testing confirms secure logon/logout functionality; application password management; user provisioning; any identity proofing; and account recovery. |
| Authorization/Access Control | This is a broad area that will include testing for privilege escalation; unauthorized file uploads; unnecessary HTTP methods; bypassing controls or application logic; and forcing application behavior. |
| Database | Testing focuses on whether queries execute securely. It should be determined if any dynamic SQL is in use and whether queries are properly parameterized to mitigate SQL injection. Various automated tools should be used, whether for a traditional RDBMS or NoSQL database, to check for vulnerabilities. Sample queries should also be requested and examined manually to identify any coding deficiencies that might identify a vulnerability. |
| Infrastructure | Testing confirms if application tiers are securely segregated from each other; whether the application is deployed in accordance with the <Organization> Technical Reference Architecture (TRA); and whether an exploitation in one tier can adversely affect another tier. |
| Input Validation | These tests focus on whether an application will accept incorrect data length, type, range, and format in form fields to observe application behavior. |
| Auditing | Auditing within the application confirms that application logs are sent to a central logging capability; that major application functions (*e.g.,* login, logout, password resets, invalid passwords, account suspension/recovery, session termination) are recorded; that sufficient information is stored with each logging event; that log files are stored in accordance with organizational requirements; and that security staff are reviewing logs for anomalies. |
| Error Handling | Testing focuses on producing error messages to confirm that error messages are not verbose in nature, revealing any information an adversary can use to exploit the system. |
| Vulnerability Identification | While vulnerabilities such as Injection and XSS must be tested for during the ACT, vulnerability testing should never be limited to just common vulnerabilities since the threat landscape is broad and dynamic. The OWASP Top 10 offers solid guidelines to begin testing, but vulnerability testing must extend well beyond the issues identified in this list. It is expected that the issues identified by OWASP will be tested for during the ACT, at a minimum. |
| Patch Management | The various components that comprise an application, such as the web server and any 3rd-party software, are evaluated to ensure the latest versions are installed. |

##### Tracking

During the assessment phase, the Application Assessor should discuss any findings with system stakeholders during daily assessment briefings, so system support staff are introduced to the findings and supporting evidence. This will ensure proper identification and tracking of findings in a POA&M through closure. It is encouraged for closure evidence to be presented and reviewed by the Application Assessor during the assessment phase, however, all testing and change control procedures must be adhered to as this could result in a finding. If closure evidence is confirmed, the finding should not be removed from the final report during the reporting phase and instead be marked as “closed” if the Application Assessor determines that the provided evidence is adequate to close the finding.

##### Tools

The Assessment Team will use a variety of system-appropriate tools in the course of technical testing. The table below lists tools that are commonly used in ACT assessments – other tools not listed here might be used, as well, on a case-by-case basis.

Table . Assessment Tools

|  |  |
| --- | --- |
| **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. |
| [InSpec](http://inspec.io/) | Open-source testing framework for infrastructure with a human- and machine-readable language for specifying compliance, security, and policy requirements. |
| [GoBuster](https://github.com/OJ/gobuster) | GoBuster is a tool used to brute-force: URIs (directories and files) in web sites; DNS subdomains (with wildcard support); and Virtual Host names on target web servers. |
| [Maltego](https://www.paterva.com/) | Maltego is an interactive data mining tool that renders directed graphs for link analysis. The tool is used in online investigations for finding relationships between pieces of information from various sources located on the Internet. |
| [Mozilla Firefox Web Browser](http://www.mozilla.org/) | Open-source Web-based browsers used to manually browse and inspect the Web application and associated forms with useful add-ons for exploitation/inspection. |
| [Nessus](http://www.nessus.org/) | Open-source vulnerability scanner and assessment tool. |
| [NetSparker](http://www.netsparker.com/) | Multi-user web security scanner with built-in workflow and reporting tools. |
| [Nmap](https://nmap.org/download.html) | Nmap, short for Network Mapper, is a free, open-source tool for vulnerability scanning and network discovery. Network administrators use Nmap to identify what devices are running on their systems, discovering hosts that are available and the services they offer, finding open ports and detecting security risks. |
| [PowerSploit/PowerView](https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon) | PowerView is a PowerShell tool to gain network situational awareness on Windows domains. It contains a set of pure-PowerShell replacements for various windows "net \*" commands, which utilize PowerShell AD hooks and underlying Win32 API functions to perform useful Windows domain functionality. |
| SCAP Compliance Checker (SCC) & CIS CAT PRO | SCC and CIS CAT PRO allow the comparison of systems against various baseline standards. These include CIS level 1, level 2, and DISA STIGs.  *Note: Require memberships to MAX.gov and CIS for download.* |
| [Sn1per](https://github.com/1N3/Sn1per) | Sn1per is an automated scanner that can be used during a penetration test to enumerate and scan for vulnerabilities. Sn1per Professional is Xero Security's premium reporting addon for Professional Penetration Testers, Bug Bounty Researchers and Corporate Security teams to manage large environments and pen test scopes. |
| [Veracode Static Analysis](https://www.veracode.com/products/binary-static-analysis-sast) | Static code analysis tool. Provides automated security feedback in the IDE and the pipeline, and conducts a full policy scan before deployment. It then provides clear guidance on what issues to focus on and how to fix them faster. |
| [W3af](https://github.com/andresriancho/w3af/) | w3af is an open-source web application security scanner which helps developers and penetration testers identify and exploit vulnerabilities in their web applications.  The scanner is able to identify 200+ vulnerabilities, including Cross-Site Scripting, SQL injection and OS commanding. |
| [WeirdAAL](https://github.com/carnal0wnage/weirdAAL) | WeirdAAL is an AWS penetration testing framework that allows enumeration of various services such as AWS lambda and IAM based modules. |
| [wget](http://www.gnu.org/software/wget/wget.html) | Open-source network tool that retrieves files from the Internet using HTTP, Secure Hyper Text Transfer Protocol (HTTPS), and the File Transfer Protocol (FTP). |
| [Wireshark](http://www.wireshark.org/) | Open-source, GUI network packet and protocol analyzer. |
| [Zed Attack Proxy (ZAP)](https://www.zaproxy.org/) | Open-source web application scanner. |

#### Conduct Application Interview

The system stakeholders (*e.g.,* System developers, ISSO) should provide an overview of their roles and responsibilities related to the application or system, as well as the controls in place to secure it. The overview should include all components for which they have a specific responsibility to ensure security in relation to the application or system. Interview guidance can be found in the Questionnaire-Application document (see Section 3 *Attachments*).

#### Consult with Other Assessors

The ACT Assessment Team performs as an integrated and cohesive team. Findings identified in respective assessment areas, such as Network, Operating System, Database, and M&O, often overlap (*e.g.,* a weak I&A application module may confirm weak or non-existent processes/procedures/policies). These findings are shared within the team at least daily in preparation for the daily out-brief stakeholder meeting, but it is encouraged that findings and information are shared more often. This serves many purposes: to inform other Assessors, to confirm identified vulnerabilities are not false positives, and helps ensure the Assessors function as a team.

#### Document Findings

Application findings focus on the vulnerabilities discovered through manual testing, automated scanning and other tools, deviations from best security practices recommendations, information elicited in interviews, and deficiencies in the application design, associated processes, procedures, and policies.

All findings in their respective assessment areas are documented by the ACT team to ensure tracking and eventual closure by the system staff. Findings are presented during the daily out-brief call and are typically confirmed with system personnel prior to the call. These findings are considered *draft* findings until confirmed. If a High or Critical severity finding is discovered by the Assessment Team, the Security Assessment Lead will immediately notify the CRA and arrange for a meeting with the appropriate stakeholders, typically the CRA, BO, and system personnel, responsible for the affected system component or process. If it is later determined that a finding is a false positive, it will remain as reported and documented as such.

### Database Assessor

Security Assessment: This role is required when database testing or assessment is required.

Summary of Database Assessor responsibilities:

* Determine whether the assertions made in documentation and interviews are correct by ensuring that the system’s functionality is exercised in an appropriate way.
* Follow the guidance provided by each Control’s “Assessment Methods and Objects” in the current version of the <Organization’s Controls Catalog>, industry best practices, and all other relevant <Organization> guidance and directives for all technical testing.
* Discover the design, implementation, and operational flaws that could violate <Organization> IS Policies, Standards, Procedures and Guidelines; Business Partners System Security Manual (BPSSM); and other standards (where applicable).
* Assess the susceptibility of the system to insider-, intranet-, Internet-, and network-based attacks.
* Review existing POA&Ms, as directed by <Organization>.
* Ensure adequate testing of every in-scope capability and sub-capability (and corresponding controls and control enhancements) in the <Organization’s Controls Catalog>.
* Verify all control inheritance assertions and document any issues with inheritance.
* Ensure that reviews of configurations and settings are performed either in Production or in a non-production environment that is a copy of the production environment.
* To the extent possible, the Assessor shall work with <Organization> and support contractors to use existing scan results from available tools. The Assessor shall review the scan configuration, ensure scans are credentialed where applicable, and ensure scans include all assets in scope.
* Use assessment tools that are acceptable to the GTL.

The Database Assessor is responsible for examining the database configuration for the various databases that are part of the system, including but not limited to Oracle, SQL Server, and MySQL databases. Responsibilities include: attaining an accurate understanding of how the database(s) support the system; using automated tools to scan the database server(s) to identify vulnerabilities and export running configurations; performing an analysis of the implemented database baselines; identifying deviations from best security practices; recording findings and consulting with other Assessors and the assessment lead to verify/corroborate findings; writing findings for the daily briefing; interviewing database administrators; and presenting database findings during the daily stakeholder briefing.

This section serves as practical guidance for individuals conducting the database evaluation for <Organization> ACT assessments. This section focuses on testing and evaluation techniques to address controls related to database testing from a technical configuration perspective.

This section assumes the Database Assessors understand the target database platform, the supporting operating system environment, and database security concepts. In addition, Database Assessors may reference and make use of vendor, government, and industry best practices and recommendations.

#### Review Documentation, Script Output, and Configs

During the planning phase, the Database Assessor reviews the Assessment Plan to understand the scope of the assessment. Based on the scope, security policies and procedures in accordance with <Organization> security requirements are reviewed. In preparation for the assessment phase, the Database Assessor will review provided documentation and script output to increase familiarity with the target system and database. The Database Assessor will determine any technical scripts, scans, or other requests to be made to ensure that the assessment period runs cleanly. During this time, any special requests for testing are provided to the ACT Security Assessment Lead or Risk Assessment Lead for coordination with the system’s Point of Contact (POC) and any applicable <Organization> representatives (ex. CRA, GTL).

The ACT Security Assessment Lead or Risk Assessment Lead will provide the system POC with any applicable database assessment script(s) and execution instructions to be run in the target database environment prior to the assessment phase. To prepare for an assessment, the Database Assessor reviews provided documentation. Available documentation *may include but is not limited to* the following (which should be requested):

* System Security Plan (SSP)
* Baseline configuration documents for each database
* Risk Assessment (RA)
  + Risk Acceptance Letters
* Policy documents, such as listed below:
  + User Administration policy
  + Password change policy
  + Audit log retention and review policy
  + Backup procedures and policy
* Configuration Management (CM) policy document
  + Change Management policy document
* Database Environment Information
  + Assessment test script output (SQL Server, Oracle, etc.)
  + A copy of Directories/Files ownership and permissions

During the assessment phase, assessment activities include documentation review, database tool output review, and personnel interviews. The database assessment tools gather information about the database installation that includes instance and configuration settings and parameters. The Database Assessor will review documents provided by the organization. The review will assess whether the system documentation adequately describes implemented security controls and augments technical security control implementations. As a part of the assessment, the Database Assessor will evaluate documentation such as, but not limited to the SSP, ISRA, CP, POA&M, Risk Acceptance Letter(s), and baseline configuration documents in accordance with organizational guidelines and identify any discovered issues or concerns.

The Database Assessor must assess the organization’s implementation of the database and database architecture to identify vulnerabilities. The database assessment script output includes information from the database that identifies potential security issues and concerns. The Database Assessor must be familiar with the <Organization> security guidance, including the <Organization’s Controls Catalog>, to effectively perform the security assessment.

In addition, the overall database environment must be evaluated. This evaluation is based upon sound database architecture principles. Issues to watch for include:

* Installation and Configuration
  + Installation and Configuration security concerns involve installed database options, ownership, file layout, file/directory permissions, listener configurations, and parameter settings
* Database Account Management
  + Database account management concerns involve password management, account permissions, and database object ownership.
* Database Access Configuration
  + Database Access Configuration security concerns involve default users and roles, public role assignment, auditing configuration, and privilege assignment.
* System Availability/Maintenance
  + System Availability/Maintenance security concerns involve backup-recovery procedures, configuration management support, and support development, test, and production application environments
* Auditing
  + Auditing security concerns involve configuring database auditing, implementing auditing procedures, following auditing guidelines and constraints

To properly evaluate the environment, the Database Assessor needs to review copies of all test tool outputs (SQL, Oracle, etc.). The files and directory permissions should be evaluated as well.

During the assessment phase, the Database Assessor should discuss any findings with system stakeholders during daily assessment out-briefs so system support staff are introduced to the findings and supporting evidence. This will ensure proper identification, tracking of findings and their potential closure. It is encouraged for closure evidence to be presented and reviewed by the Database Assessor during the assessment phase, however, all testing and change control procedures must be adhered to as this could result in a finding. If closure evidence is confirmed, the finding should not be removed from the final report during the reporting phase and instead be marked as “closed” if the Database Assessor determines that the provided evidence is adequate to close the finding.

#### Conduct Database Interview

The system stakeholders (*e.g.,* database administrator, ISSO) should provide an overview of their roles and responsibilities related to the application or system, as well as the controls in place to secure it. The overview should include all components for which they have a specific responsibility to ensure security in relation to the application or system. Interview guidance can be found in the Questionnaire-Database document (see Section 3 *Attachments*).

#### Consult with Other Assessors

The ACT Assessment Team performs as an integrated and cohesive team. Findings identified in respective assessment areas, such as Network, Operating System, Application, and M&O, often overlap (*e.g.,* a weak baseline configuration for the database may confirm weak or non-existent database processes/procedures/policies). These findings are shared within the team at least daily in preparation for the daily out-brief stakeholder meeting, but it is encouraged that findings and information are shared more often. This serves many purposes: to inform other Assessors, to confirm identified vulnerabilities are not false positives, and helps ensure the Assessors function as a team.

#### Document Findings

Database findings focus on the vulnerabilities discovered through automated scanning, deviations from best practices baseline configuration recommendations, information elicited in interviews, and deficiencies in the associated processes, procedures, and policies.

All findings in their respective assessment areas are documented by the ACT team to ensure tracking and eventual closure by the system staff. Findings are presented during the daily out-brief call and are typically confirmed with system personnel prior to the call. These findings are considered *draft* findings until confirmed. If a High or Critical severity finding is discovered by the Assessment Team, the Security Assessment Lead will immediately notify the CRA and arrange for a meeting with the appropriate stakeholders, typically the CRA, BO, and system personnel, responsible for the affected system component or process. If it is later determined that a finding is a false positive, it will remain as reported and documented as such.

### Operating System Assessor

Security Assessment: This role is required when operating system testing or assessment is required.

Summary of Operating System Assessor responsibilities:

* Determine whether the assertions made in documentation and interviews are correct by exercising and testing the system’s functionality.
* Follow the guidance provided by each Control’s “Assessment Methods and Objects” in the current version of the <Organization’s Controls Catalog>, industry best practices, and all other relevant <Organization> guidance and directives for all technical testing.
* Discover the design, implementation, and operational flaws that could violate <Organization> IS Policies, Standards, Procedures and Guidelines; Business Partners System Security Manual (BPSSM); and other standards (where applicable).
* Assess the susceptibility of the system to insider-, intranet-, Internet-, and network-based attacks.
* Review existing POA&Ms, as directed by <Organization>.
* Ensure adequate testing of every in-scope capability and sub-capability (and corresponding controls and control enhancements) in the <Organization’s Controls Catalog>.
* Verify all control inheritance assertions and document any issues with inheritance.
* Ensure that reviews of configurations and settings are performed either in Production or in a non-production environment that is a copy of the production environment.
* To the extent possible, the Assessor shall work with <Organization> and support contractors to use existing scan results from available tools. The Assessor shall review the scan configuration, ensure scans are credentialed where applicable, and ensure scans include all assets in scope.
* Use assessment tools that are acceptable to the GTL.

The Operating System (OS) Assessor is responsible for examining the OS configuration for the various operating systems that are part of the General Support System (GSS), including but not limited to Windows and Linux OS’s. Responsibilities include: attaining an accurate understanding of how the servers support the system—whether database or application servers, for example; using automated tools to scan the servers to identify vulnerabilities and export running configurations; performing an analysis of the implemented server baselines; identifying deviations from best security practices; recording findings and consulting with other Assessors and the assessment lead to verify/corroborate findings; writing findings for the daily briefing; interviewing OS system administrators; and presenting OS findings during the daily stakeholder briefing.

This section serves as practical guidance for individuals conducting the OS security evaluation for <Organization> ACT assessments. This section focuses on testing and evaluation techniques to address controls related to OS testing from a technical configuration perspective.

This section assumes OS Assessors understand Windows and Linux OS’s, the supporting operating system environment, and OS security concepts.

#### Review Documentation, Script Output, and Configs

During the planning phase, the OS Assessor reviews the ACT Assessment Plan to understand the scope of the assessment. Based on the scope, security policies and procedures in accordance with <Organization> security requirements are reviewed. In preparation for the assessment phase, the OS Assessor will review provided documentation and script output (*e.g.,* Windows / Linux) to increase familiarity with the target system and OS. The OS Assessor will identify any technical scripts, scans, or other requests to be made to ensure that the assessment period runs smoothly. During this time, any special requests for testing are provided to the ACT Security Assessment Lead or Risk Assessment Lead for coordination with the system’s Point of Contact (POC) and any applicable <Organization> representatives (*e.g.,* system administrators, ISSO).

The ACT Security Assessment Lead or Risk Assessment Lead will provide the system POC with any applicable OS assessment script(s) and execution instructions to be run in the target environment prior to the assessment phase. To prepare for an assessment, the OS Assessor reviews provided documentation. Available documentation *may include but is not limited to* the following (which should be requested):

* System Security Plan (SSP)
* Baseline configuration documents for each OS
* Information Security Risk Assessment (ISRA)
* Plan of Action and Milestones (POA&M)
* Policy documents, such as:
  + User Administration policy
  + Password change policy
  + Audit log retention and review policy
  + Backup procedures and policy
* Configuration Management (CM) policy document
  + Change Management policy document
* OS Environment Information
  + Assessment test script output
  + OS inventory
  + Group Policy Object (GPO) exports for Windows
  + Vulnerability scan results

During the assessment phase, the OS Assessor must assess the organization’s implementation of the deployed OS’s to identify vulnerabilities. Assessment activities include documentation review, OS script and vulnerability scan output review, and personnel interviews.

The OS assessment script output includes information from the OS that identifies potential security issues and concerns in relation to a best practices security baseline. The OS Assessor must be familiar with the <Organization> security guidance, including the <Organization’s Controls Catalog>, to effectively perform the OS assessment. An export of any GPOs is also requested to facilitate examination of the implemented OS configuration against best practices.

Vulnerability scan results, from a tool like Nessus, for example, also provide valuable information on the implemented OS configuration, obsolete software, required patches, and any Common Vulnerabilities and Exposures (CVEs) that have been identified. OS Assessors should correlate scan results with other OS information sources, such as script output, GPO exports, and information elicited in OS interviews, to ensure that any false positives can be eliminated.

Additionally, the overall OS environment must be evaluated. The assessment is based upon accepted best practices guidance. Issues to watch for include:

* Installation and Configuration
  + Installation and configuration security concerns involve default OS installation settings and adherence to best practices baselines.
* OS Account Management
  + OS account management concerns involve default users and roles, role and privilege assignment, and password management.
* System Availability/Maintenance
  + System availability/maintenance security concerns involve backup-recovery procedures, configuration management support, and support to the development, test, and production application environments.
* Auditing
  + Auditing security concerns involve configuration of automated logging, identifying whether a centralized logging capability exists, implementing auditing procedures, and following auditing guidelines and constraints.

#### Conduct Operating System(s) Interview

The system stakeholders (*e.g.,* OS administrator, ISSO) should provide an overview of their roles and responsibilities related to the application or system, as well as the controls in place to secure it. The overview should include all components for which they have a specific responsibility to ensure security in relation to the application or system. Interview guidance can be found in the Questionnaire-Networks and Operating Systems document (see Section 3 *Attachments*).

#### Consult with Other Assessors

The ACT Assessment Team performs as an integrated and cohesive team. Findings identified in respective assessment areas, such as Network, Database, Application, and M&O, often overlap (*e.g.,* a weak baseline configuration for the OS may confirm weak or non-existent OS processes/procedures/policies). These findings are shared within the team at least daily in preparation for the daily out-brief stakeholder meeting, but it is encouraged that findings and information are shared more often. This serves many purposes: to inform other Assessors, to confirm identified vulnerabilities are not false positives, and helps ensure the Assessors function as a team.

#### Document Findings

Operating System findings focus on the vulnerabilities discovered through automated scanning and other tools, deviations from best practices configuration recommendations, information elicited in interviews, and deficiencies in the associated processes, procedures, and policies.

All findings in their respective assessment areas are documented by the ACT team to ensure tracking and eventual closure by the system staff. Findings are presented during the daily out-brief call and are typically confirmed with system personnel prior to the call. These findings are considered *draft* findings until confirmed. If a High or Critical severity finding is discovered by the Assessment Team, the Security Assessment Lead will immediately notify the CRA and arrange for a meeting with the appropriate stakeholders, typically the CRA, BO, and system personnel, responsible for the affected system component or process. If it is later determined that a finding is a false positive, it will remain as reported and documented as such.

### Virtualization Assessor

Security Assessment: This role is required when virtualization testing or assessment is required.

Summary of Virtualization Assessor responsibilities:

* Determine whether the assertions made in documentation and interviews are correct by exercising and testing the system’s functionality.
* Follow the guidance provided by each Control’s “Assessment Methods and Objects” in the current version of the NIST SP 800-53, industry best practices, and all other relevant <Organization> guidance and directives for all technical testing.
* Discover the design, implementation, and operational flaws that could violate <Organization> policies, standards, procedures, and guidelines (where applicable).
* Assess the susceptibility of the system to insider-, intranet-, Internet-, and network-based attacks.
* Review existing POA&Ms, as directed by <Organization>.
* Ensure adequate testing of every in-scope capability and sub-capability (and corresponding controls and control enhancements) in the NIST SP 800-53.
* Verify all control inheritance assertions and document any issues with inheritance.
* Ensure that reviews of configurations and settings are performed either in Production or in a non-production environment that is a copy of the production environment.
* To the extent possible, the Assessor shall work with <Organization> and support contractors to use existing scan results from available tools. The Assessor shall review the scan configuration, ensure scans are credentialed where applicable, and ensure scans include all assets in scope.
* Use assessment tools that are acceptable to the GTL.

The Virtualization Assessor is responsible for examining the configuration for the various hypervisors and virtualization infrastructure that are part of the system or of the General Support System (GSS). Responsibilities include: attaining an accurate understanding of how virtualization supports the system; using automated tools to scan the virtualization infrastructure to identify vulnerabilities and export running configurations; performing an analysis of the implemented virtualization baselines; identifying deviations from best security practices; recording findings and consulting with other Assessors and the assessment lead to verify/corroborate findings; writing findings for the daily briefing; interviewing virtualization system administrators; and presenting virtualization findings during the daily stakeholder briefing.

This section serves as practical guidance for individuals conducting the virtualization security evaluation for <Organization> ACT assessments. This section focuses on testing and evaluation techniques to address controls related to virtualization testing from a technical configuration perspective.

This section assumes Virtualization Assessors understand general virtualization concepts and technologies, as well as the specific virtualization technologies being assessed.

#### Review Documentation, Script Output, and Configs

During the planning phase, the Virtualization Assessor reviews the ACT Assessment Plan to understand the scope of the assessment. Based on the scope, security policies and procedures in accordance with <Organization> security requirements are reviewed. In preparation for the assessment phase, the Virtualization Assessor will review provided documentation and script output to increase familiarity with the target system and virtualization technologies. The Virtualization Assessor will identify any technical scripts, scans, or other requests to be made to ensure that the assessment period runs smoothly. During this time, any special requests for testing are provided to the ACT Security Assessment Lead or Risk Assessment Lead for coordination with the system’s Point of Contact (POC) and any applicable <Organization> representatives (*e.g.,* system administrators, ISSO).

The ACT Security Assessment Lead or Risk Assessment Lead will provide the system POC with any applicable virtualization assessment script(s) and execution instructions to be run in the target environment prior to the assessment phase. To prepare for an assessment, the Virtualization Assessor reviews provided documentation. Available documentation *may include but is not limited to* the following (which should be requested):

* System Security Plan (SSP)
* Baseline configuration documents for each virtualization technology
* Information Security Risk Assessment (ISRA)
* Plan of Action and Milestones (POA&M)
* Policy documents, such as:
  + User Administration policy
  + Password change policy
  + Audit log retention and review policy
  + Backup procedures and policy
* Configuration Management (CM) policy document
  + Change Management policy document
* OS Environment Information
  + Assessment test script output
  + Virtualization infrastructure inventory
  + Group Policy Object (GPO) exports for Windows
  + Vulnerability scan results

During the assessment phase, the Virtualization Assessor must assess the organization’s implementation of the deployed virtualization infrastructure to identify vulnerabilities. Assessment activities include documentation review, virtualization script and vulnerability scan output review, and personnel interviews.

The Virtualization assessment script output includes information from the virtualization infrastructure that identifies potential security issues and concerns in relation to a best practices security baseline. The Virtualization Assessor must be familiar with the <Organization> security guidance, including the NIST SP 800-53, to effectively perform the virtualization assessment.

Vulnerability scan results, from a tool like Nessus, for example, also provide valuable information on the implemented virtualization infrastructure configuration, obsolete software, required patches, and any Common Vulnerabilities and Exposures (CVEs) that have been identified. Virtualization Assessors should correlate scan results with other virtualization information sources, such as script output and information elicited in virtualization interviews, to ensure that any false positives can be eliminated.

Additionally, the overall virtualization environment must be evaluated. The assessment is based upon accepted best practices guidance. Issues to watch for include:

* Installation and Configuration
  + Installation and configuration security concerns involve default virtualization installation settings and adherence to best practices baselines.
* Virtualization Account Management
  + Virtualization account management concerns involve default users and roles, role and privilege assignment, and password management.
* System Availability/Maintenance
  + System availability/maintenance security concerns involve backup-recovery procedures, configuration management support, and support to the development, test, and production application environments.
* Auditing
  + Auditing security concerns involve configuration of automated logging, identifying whether a centralized logging capability exists, implementing auditing procedures, and following auditing guidelines and constraints.

#### Conduct Virtualization Interview

The system stakeholders (*e.g.,* virtualization administrator, ISSO) should provide an overview of their roles and responsibilities related to the application or system, as well as the controls in place to secure it. The overview should include all components for which they have a specific responsibility to ensure security in relation to the application or system. Interview guidance can be found in the Questionnaire-Virtualization document (see Section 3 *Attachments*).

#### Consult with Other Assessors

The ACT Assessment Team performs as an integrated and cohesive team. Findings identified in respective assessment areas, such as Network, Database, Application, and M&O, often overlap (*e.g.,* a weak baseline configuration for the virtualization infrastructure may confirm weak or non-existent virtualization processes/procedures/policies). These findings are shared within the team at least daily in preparation for the daily out-brief stakeholder meeting, but it is encouraged that findings and information are shared more often. This serves many purposes: to inform other Assessors, to confirm identified vulnerabilities are not false positives, and helps ensure the Assessors function as a team.

#### Document Findings

Virtualization findings focus on the vulnerabilities discovered through automated scanning and other tools, deviations from best practices configuration recommendations, information elicited in interviews, and deficiencies in the associated processes, procedures, and policies.

All findings in their respective assessment areas are documented by the ACT team to ensure tracking and eventual closure by the system staff. Findings are presented during the daily out-brief call and are typically confirmed with system personnel prior to the call. These findings are considered *draft* findings until confirmed. If a High or Critical severity finding is discovered by the Assessment Team, the Security Assessment Lead will immediately notify the CRA and arrange for a meeting with the appropriate stakeholders, typically the CRA, SO, and system personnel, responsible for the affected system component or process. If it is later determined that a finding is a false positive, it will remain as reported and documented as such.

### Mainframe Assessor

Security Assessment: This role is required when mainframe testing or assessment is required.

Summary of Mainframe Assessor responsibilities:

* Determine whether the assertions made in documentation and interviews are correct by exercising and testing the system’s functionality.
* Follow the guidance provided by each Control’s “Assessment Methods and Objects” in the current version of the NIST SP 800-53, industry best practices, and all other relevant <Organization> guidance and directives for all technical testing.
* Discover the design, implementation, and operational flaws that could violate <Organization> policies, standards, procedures, and guidelines (where applicable).
* Assess the susceptibility of the system to insider-, intranet-, Internet-, and network-based attacks.
* Review existing POA&Ms, as directed by <Organization>.
* Ensure adequate testing of every in-scope capability and sub-capability (and corresponding controls and control enhancements) in the NIST SP 800-53.
* Verify all control inheritance assertions and document any issues with inheritance.
* Ensure that reviews of configurations and settings are performed either in Production or in a non-production environment that is a copy of the production environment.
* To the extent possible, the Assessor shall work with <Organization> and support contractors to use existing scan results from available tools. The Assessor shall review the scan configuration, ensure scans are credentialed where applicable, and ensure scans include all assets in scope.
* Use assessment tools that are acceptable to the GTL.

The Mainframe Assessor is responsible for examining the configuration for the mainframe operating system that is part of the General Support System (GSS). Responsibilities include: attaining an accurate understanding of how the mainframe supports the system; performing manual testing; using automated tools, if possible, to scan the mainframe to identify vulnerabilities; performing an analysis of the implemented mainframe security baseline; identifying deviations from best security practices; recording findings and consulting with other Assessors and the assessment lead to verify/corroborate findings; writing findings for the daily briefing; interviewing mainframe system administrators; and presenting mainframe findings during the daily stakeholder briefing.

This section serves as practical guidance for individuals conducting the mainframe evaluation for <Organization> ACT assessments. This section focuses on testing and evaluation techniques to address controls related to mainframe testing from a technical configuration perspective.

This section assumes Mainframe Assessors understand mainframe architecture, the mainframe OS, and mainframe security concepts.

#### Review Documentation, Script Output, and Configs

During the planning phase, the Mainframe Assessor reviews the ACT Assessment Plan to understand the scope of the assessment. Based on the scope, security policies and procedures in accordance with <Organization> security requirements are reviewed. In preparation for the assessment phase, the Mainframe Assessor will review provided documentation and any script output to increase familiarity with the target system. The Mainframe Assessor will identify any technical scripts, scans, or other requests to be made to ensure that the assessment period runs smoothly. During this time, any special requests for testing are provided to the ACT Security Assessment Lead or Risk Assessment Lead for coordination with the system’s Point of Contact (POC) and any applicable <Organization> representatives (*e.g.,* mainframe administrators, ISSO).

The ACT Security Assessment Lead or Risk Assessment Lead will provide the system POC with any applicable mainframe assessment script(s) and execution instructions to be run in the target environment prior to the assessment phase. To prepare for an assessment, the Mainframe Assessor reviews provided documentation. Available documentation *may include but is not limited to* the following (which should be requested):

* System Security Plan (SSP)
* Baseline configuration documents for mainframe OS
* Information Security Risk Assessment (ISRA)
* Plan of Action and Milestones (POA&M)
* Policy documents, such as:
  + User Administration policy
  + Password change policy
  + Audit log retention and review policy
  + Backup procedures and policy
* Configuration Management (CM) policy document
  + Change Management policy document
* Mainframe Environment Information
  + Assessment test script output (if applicable)
  + Mainframe architecture diagram
  + Vulnerability scan results (if applicable)

During the assessment phase, the Mainframe Assessor must assess the organization’s implementation of the mainframe to identify vulnerabilities. Assessment activities include documentation review, OS script and vulnerability scan output review, and personnel interviews.

Any mainframe assessment script output includes information from the mainframe that identifies potential security issues and concerns in relation to a best practices security baseline. The Mainframe Assessor must be familiar with the <Organization> security guidance, including the NIST SP 800-53, to effectively perform the mainframe assessment.

Vulnerability scan results, from a tool like Nessus, for example, also provide valuable information on the implemented mainframe OS configuration, obsolete software, required patches, and any Common Vulnerabilities and Exposures (CVEs) that have been identified. Mainframe Assessors should correlate scan results with other mainframe information sources, such as script output, and information elicited in mainframe interviews, to ensure that any false positives can be eliminated.

Additionally, the overall mainframe environment must be evaluated. The assessment is based upon accepted best practices guidance. Issues to watch for include:

* Installation and Configuration
  + Installation and configuration security concerns involve default mainframe OS installation settings and adherence to best practices baselines.
* Account Management
  + Mainframe OS account management concerns involve default users and roles, role and privilege assignment, and password management.
* System Availability/Maintenance
  + System availability/maintenance security concerns involve backup-recovery procedures, configuration management support, and support to the development, test, and production application environments.
* Auditing security concerns involve configuration of automated logging, identifying whether a centralized logging capability exists, implementing auditing procedures, and following auditing guidelines and constraints.

#### Conduct Mainframe Interview

The system stakeholders (*e.g.,* Mainframe system administrator, ISSO) should provide an overview of their roles and responsibilities related to the application or system, as well as the controls in place to secure it. The overview should include all components for which they have a specific responsibility to ensure security in relation to the application or system. Interview guidance can be found in the Questionnaire-Mainframe document (see Section 3 *Attachments*).

#### Consult with Other Assessors

The ACT Assessment Team performs as an integrated and cohesive team. Findings identified in respective assessment areas, such as Network, Operating System, Application, and M&O, often overlap (*e.g.,* a weak baseline configuration for the mainframe OS may confirm weak or non-existent processes/procedures/policies). These findings are shared within the team at least daily in preparation for the daily out-brief stakeholder meeting, but it is encouraged that findings and information are shared more often. This serves many purposes: to inform other Assessors, to confirm identified vulnerabilities are not false positives, and helps ensure the Assessors function as a team.

#### Document Findings

Mainframe findings focus on the vulnerabilities discovered through manual examination, tool output, deviations from best practices baseline configuration recommendations, information elicited in interviews, and deficiencies in the associated processes, procedures, and policies.

All findings in their respective assessment areas are documented by the ACT team to ensure tracking and eventual closure by the system staff. Findings are presented during the daily out-brief call and are typically confirmed with system personnel prior to the call. These findings are considered *draft* findings until confirmed. If a High or Critical severity finding is discovered by the Assessment Team, the Security Assessment Lead will immediately notify the CRA and arrange for a meeting with the appropriate stakeholders, typically the CRA, SO, and system personnel, responsible for the affected system component or process. If it is later determined that a finding is a false positive, it will remain as reported and documented as such.

### Network Assessor

Security Assessment: This role is required when network device testing or assessment is required.

Summary of Network Assessor responsibilities:

* Determine whether the assertions made in documentation and interviews are correct by exercising and testing the system’s functionality.
* Follow the guidance provided by each Control’s “Assessment Methods and Objects” in the current version of the NIST SP 800-53, industry best practices, and all other relevant <Organization> guidance and directives for all technical testing.
* Discover the design, implementation, and operational flaws that could violate policies, standards, procedures, and guidelines (where applicable).
* Assess the susceptibility of the system to insider-, intranet-, Internet-, and network-based attacks.
* Review existing POA&Ms, as directed by <Organization>.
* Ensure adequate testing of every in-scope capability and sub-capability (and corresponding controls and control enhancements) in the NIST SP 800-53.
* Verify all control inheritance assertions and document any issues with inheritance.
* Ensure that reviews of configurations and settings are performed either in Production or in a non-production environment that is a copy of the production environment.
* To the extent possible, the Assessor shall work with <Organization> and support contractors to use existing scan results from available tools. The Assessor shall review the scan configuration, ensure scans are credentialed where applicable, and ensure scans include all assets in scope.
* Use assessment tools that are acceptable to the GTL.

The Network Assessor is responsible for examining the network architecture and configuration of the various network appliance (*e.g.,* firewalls, switches, routers) operating systems that are part of the General Support System (GSS). Responsibilities include: attaining an accurate understanding of the network architecture design; using automated tools to scan network appliances to identify vulnerabilities and export running configurations; examining and performing an analysis of automated tool output; identifying deviations from best network security practices; recording findings and consulting with other Assessors and the assessment lead to verify/corroborate findings; writing findings for the daily briefing; interviewing network system staff; and presenting network findings during the daily stakeholder briefing.

This section serves as practical guidance for individuals conducting the network evaluation for <Organization> ACT assessments. This section focuses on testing and evaluation techniques to address controls related to network testing from a technical configuration perspective.

This section assumes Network Assessors understand network architecture, network appliance OS’s, and network security concepts.

#### Review Documentation, Script Output, and Configs

During the planning phase, the Network Assessor reviews the ACT Assessment Plan to understand the scope of the assessment. Based on the scope, security policies and procedures in accordance with <Organization> security requirements are reviewed. In preparation for the assessment phase, the Network Assessor will review provided documentation and network appliance running configurations to increase familiarity with the network environment. The Network Assessor will identify any technical scripts, scans, or other requests to be made to ensure that the assessment period runs smoothly. During this time, any special requests for testing are provided to the ACT Security Assessment Lead or Risk Assessment Lead for coordination with the system’s Point of Contact (POC) and any applicable <Organization> representatives (*e.g.,* network administrators, ISSO).

The ACT Security Assessment Lead or Risk Assessment Lead will provide the system POC with any applicable network data calls and execution instructions to be run in the target environment prior to the assessment phase. To prepare for an assessment, the Network Assessor reviews provided documentation. Available documentation *may include but is not limited to* the following (which should be requested):

* System Security Plan (SSP)
* Baseline configuration documents for each network appliance OS
* Information Security Risk Assessment (ISRA)
* Plan of Action and Milestones (POA&M)
* Policy documents, such as:
  + Network Administration policy
  + Password change policy
  + Remote access policy
  + Audit log retention and review policy
* Configuration Management (CM) policy document
  + Change Management policy document
* Network Environment Information
  + Data call output
  + Network architecture diagrams
  + Network appliance inventory
  + Vulnerability scan results

During the assessment phase, the Network Assessor must assess the organization’s implementation of the deployed network appliances to identify vulnerabilities. Assessment activities include documentation/architecture review, data call and vulnerability scan output review, and network personnel interviews.

The data call output includes information from the network appliances that identifies potential security issues and concerns in relation to a best practices security baseline. The Network Assessor must be familiar with the <Organization> security guidance, including the NIST SP 800-53, to effectively perform the network assessment.

Vulnerability scan results, from a tool like Nessus, for example, also provide valuable information on the implemented network appliance configuration, obsolete software, required patches, and any Common Vulnerabilities and Exposures (CVEs) that have been identified. Network Assessors should correlate scan results with other information sources, such as script and other data call output, and information elicited in network interviews, to ensure that any false positives can be eliminated.

Additionally, the overall network environment must be evaluated. The assessment is based upon accepted best practices guidance. Issues to watch for include:

* Installation and Configuration
  + Installation and configuration security concerns involve default network appliance OS installation settings, adherence to best practices baselines, and proper network segmentation.
* Account Management
  + Account management concerns involve default users and roles, role and privilege assignment, and password management on network appliances.
* System Availability/Maintenance
  + System availability/maintenance security concerns involve backup-recovery procedures, configuration management support, and support to the development, test, and production application environments.
* Auditing
  + Auditing security concerns involve configuration of automated logging, identifying whether a centralized logging capability exists, implementing auditing procedures, and following network auditing guidelines and constraints.

#### Conduct Network Interview

The system stakeholders (*e.g.,* Network administrator, ISSO) should provide an overview of their roles and responsibilities related to the application or system, as well as the controls in place to secure it. The overview should include all components for which they have a specific responsibility to ensure security in relation to the application or system. Interview guidance can be found in the Questionnaire-Networks and Operating Systems document (see Section 3 *Attachments*).

#### Consult with Other Assessors

The ACT Assessment Team performs as an integrated and cohesive team. Findings identified in respective assessment areas, such as Database, Operating System, Application, and M&O, often overlap (*e.g.,* a weak baseline configuration for the network appliances may confirm weak or non-existent network processes/procedures/policies). These findings are shared within the team at least daily in preparation for the daily out-brief stakeholder meeting, but it is encouraged that findings and information are shared more often. This serves many purposes: to inform other Assessors, to confirm identified vulnerabilities are not false positives, and helps ensure the Assessors function as a team.

#### Document Findings

Network findings focus on the vulnerabilities discovered through automated scanning and other tools, deviations from best practices baseline configuration recommendations, information elicited in interviews, and deficiencies in the network architecture design, associated processes, procedures, and policies.

All findings in their respective assessment areas are documented by the ACT team to ensure tracking and eventual closure by the system staff. Findings are presented during the daily out-brief call and are typically confirmed with system personnel prior to the call. These findings are considered *draft* findings until confirmed. If a High or Critical severity finding is discovered by the Assessment Team, the Security Assessment Lead will immediately notify the CRA and arrange for a meeting with the appropriate stakeholders, typically the CRA, SO, and system personnel, responsible for the affected system component or process. If it is later determined that a finding is a false positive, it will remain as reported and documented as such.

### Cloud Assessor

Security Assessment: This role is required when cloud technology testing or assessment is required.

Summary of Cloud Assessor responsibilities:

* Determine whether the assertions made in documentation and interviews are correct by exercising and testing the system’s functionality.
* Follow the guidance provided by each Control’s “Assessment Methods and Objects” in the current version of the NIST SP 800-53, industry best practices, and all other relevant <Organization> guidance and directives for all technical testing.
* Discover the design, implementation, and operational flaws that could violate <Organization> policies, standards, procedures and guidelines and other standards (where applicable).
* Assess the susceptibility of the system to insider-, intranet-, Internet-, and network-based attacks.
* Review existing POA&Ms, as directed by <Organization>.
* Ensure adequate testing of every in-scope capability and sub-capability (and corresponding controls and control enhancements) in the NIST SP 800-53.
* Verify all control inheritance assertions and document any issues with inheritance.
* Ensure that reviews of configurations and settings are performed either in Production or in a non-production environment that is a copy of the production environment.
* To the extent possible, the Assessor shall work with <Organization> and support contractors to use existing scan results from available tools. The Assessor shall review the scan configuration, ensure scans are credentialed where applicable, and ensure scans include all assets in scope.
* Use assessment tools that are acceptable to the GTL.

The Cloud Assessor is responsible for examining the cloud architecture and configuration of the various cloud technologies and components that are utilized by or incorporated into the system. Responsibilities include: attaining an accurate understanding of the cloud architecture design; using automated tools to scan cloud technologies and components to identify vulnerabilities and export running configurations; examining and performing an analysis of automated tool output; identifying deviations from best cloud security practices; recording findings and consulting with other Assessors and the assessment lead to verify/corroborate findings; writing findings for the daily briefing; interviewing cloud system staff; and presenting cloud findings during the daily stakeholder briefing.

This section serves as practical guidance for individuals conducting the cloud evaluation for <Organization> ACT assessments. This section focuses on testing and evaluation techniques to address controls related to network testing from a technical configuration perspective.

This section assumes Cloud Assessors understand cloud architecture, cloud technologies, and cloud security concepts.

#### Review Documentation, Script Output, and Configs

During the planning phase, the Cloud Assessor reviews the ACT Assessment Plan to understand the scope of the assessment. Based on the scope, security policies and procedures in accordance with <Organization> security requirements are reviewed. In preparation for the assessment phase, the Cloud Assessor will review provided documentation and cloud technologies and components to increase familiarity with the cloud environment. The Cloud Assessor will identify any technical scripts, scans, or other requests to be made to ensure that the assessment period runs smoothly. During this time, any special requests for testing are provided to the ACT Security Assessment Lead or Risk Assessment Lead for coordination with the system’s Point of Contact (POC) and any applicable <Organization> representatives (*e.g.,* cloud administrators, ISSO).

The ACT Security Assessment Lead or Risk Assessment Lead will provide the system POC with any applicable cloud data calls and execution instructions to be run in the target environment prior to the assessment phase. To prepare for an assessment, the Cloud Assessor reviews provided documentation. Available documentation *may include but is not limited to* the following (which should be requested):

* System Security Plan (SSP)
* Baseline configuration documents for each cloud technology and/or component
* Information Security Risk Assessment (ISRA)
* Plan of Action and Milestones (POA&M)
* Policy documents, such as:
  + Cloud Administration policy
  + Remote access policy
  + Audit log retention and review policy
* Configuration Management (CM) policy document
  + Change Management policy document
* Cloud Environment Information
  + Data call output
  + Cloud architecture diagrams
  + Cloud component inventory
  + Vulnerability scan results

During the assessment phase, the Cloud Assessor must assess the organization’s implementation of the deployed cloud technologies and components to identify vulnerabilities. Assessment activities include documentation/architecture review, data call and vulnerability scan output review, and cloud personnel interviews.

The data call output includes information from the cloud technologies and components that identify potential security issues and concerns in relation to a best practices security baseline. The Cloud Assessor must be familiar with <Organization> security guidance, including the NIST SP 800-53, to effectively perform the cloud assessment.

Vulnerability scan results, from a tool like Nessus (for example) also provide valuable information on the implemented cloud component configuration, obsolete software, required patches, and any Common Vulnerabilities and Exposures (CVEs) that have been identified. Cloud Assessors should correlate scan results with other information sources, such as script and other data call output, and information elicited in cloud and network interviews, to ensure that any false positives can be eliminated.

Additionally, the overall cloud environment must be evaluated. The assessment is based upon accepted best practices guidance. Issues to watch for include:

* Installation and Configuration
  + Installation and configuration security concerns involve default cloud component installation settings, adherence to best practices baselines, and proper cloud/network segmentation.
* Account Management
  + Account management concerns involve default users and roles, role and privilege assignment, and password management on network appliances.
* System Availability/Maintenance
  + System availability/maintenance security concerns involve backup-recovery procedures, configuration management support, and support to the development, test, and production application environments.
* Auditing
  + Auditing security concerns involve configuration of automated logging, identifying whether a centralized logging capability exists, implementing auditing procedures, and following network auditing guidelines and constraints.

#### Conduct Cloud Interview

The system stakeholders (*e.g.,* Cloud administrator, ISSO) should provide an overview of their roles and responsibilities related to the application or system, as well as the controls in place to secure it. The overview should include all components for which they have a specific responsibility to ensure security in relation to the application or system. Interview guidance can be found in the Questionnaire-Cloud document (see Section 3 *Attachments*).

#### Consult with Other Assessors

The ACT Assessment Team performs as an integrated and cohesive team. Findings identified in respective assessment areas, such as Database, Operating System, Application, and M&O, often overlap (*e.g.,* a weak baseline configuration for the cloud technologies may confirm weak or non-existent cloud processes/procedures/policies). These findings are shared within the team at least daily in preparation for the daily out-brief stakeholder meeting, but it is encouraged that findings and information are shared more often. This serves many purposes: to inform other Assessors, to confirm identified vulnerabilities are not false positives, and helps ensure the Assessors function as a team.

#### Document Findings

Cloud findings focus on the vulnerabilities discovered through automated scanning and other tools, deviations from best practices baseline configuration recommendations, information elicited in interviews, and deficiencies in the network architecture design, associated processes, procedures, and policies.

All findings in their respective assessment areas are documented by the ACT team to ensure tracking and eventual closure by the system staff. Findings are presented during the daily out-brief call and are typically confirmed with system personnel prior to the call. These findings are considered *draft* findings until confirmed. If a High or Critical severity finding is discovered by the Assessment Team, the Security Assessment Lead will immediately notify the CRA and arrange for a meeting with the appropriate stakeholders, typically the CRA, SO, and system personnel, responsible for the affected system component or process. If it is later determined that a finding is a false positive, it will remain as reported and documented as such.

### Privacy Assessor

Security Assessment: This role is required when privacy testing or assessment is required.

Summary of Privacy Assessor responsibilities:

* Determine whether the assertions made in documentation and interviews are correct by exercising and testing the system’s functionality.
* Follow the guidance provided by each Control’s “Assessment Methods and Objects” in the current version of the <Organization’s Controls Catalog>, industry best practices, and all other relevant <Organization> guidance and directives for all technical testing.
* Discover the design, implementation, and operational flaws that could violate <Organization> policies, standards, procedures, and guidelines (where applicable).
* Assess the susceptibility of the system to insider-, intranet-, Internet-, and network-based attacks.
* Review existing POA&Ms, as directed by <Organization>.
* Ensure adequate testing of every in-scope capability and sub-capability (and corresponding controls and control enhancements) in NIST SP 800-53.
* Verify all control inheritance assertions and document any issues with inheritance.
* Ensure that reviews of configurations and settings are performed either in Production or in a non-production environment that is a copy of the production environment.
* To the extent possible, the Assessor shall work with <Organization> and support contractors to use existing scan results from available tools. The Assessor shall review the scan configuration, ensure scans are credentialed where applicable, and ensure scans include all assets in scope.
* Use assessment tools that are acceptable to the GTL.

The Privacy Assessor is responsible for performing an analysis of the various privacy artifacts, policies, procedures, and processes to identify privacy deficiencies. Responsibilities include attaining an accurate understanding of the system architecture; reviewing core privacy artifacts, such as the PIA; identifying deviations from best privacy practices; recording findings and consulting with other Assessors and the Assessment Lead to verify/corroborate findings; writing findings for the daily briefing; interviewing privacy staff, such as the Privacy Subject Matter Expert (PSME); and presenting privacy findings during the daily stakeholder briefing.

This section is intended to serve as practical guidance for individuals conducting privacy related responsibilities for <Organization> ACT assessments. This section focuses on assessment of the privacy controls that <Organization> requires to be in place for infrastructures, systems, and applications in support of <Organization> business needs. Privacy controls involve those safeguards and countermeasures that have been implemented to manage Protected Health Information (PHI) and Personally Identifiable Information (PII) within the information system and the associated risks to <Organization> assets and operations.

During the planning phase, the Privacy Assessor reviews the Assessment Plan to understand the assessment’s scope. Based on the scope, the <Organization> security policies, requirements and procedures are reviewed to ensure an understanding of those that are applicable to the current assessment. As system documentation is received, the Privacy Assessor reviews the documentation to ensure full system knowledge in coordination with the assessment’s scope. The Privacy Assessor also determines any additional requests to ensure that the assessment period runs smoothly. During this time, any special requests are provided to the ACT Security Assessment Lead or Risk Assessment Lead so he/she can contact the system’s Point of Contact (POC) and any applicable <Organization> representatives (*e.g.,* Privacy SME) to ensure all requirements for the privacy assessment are complete.

During the assessment phase, the Privacy Assessor’s activities consist mainly of documentation review, personnel interviews, and overall analysis of implemented privacy policies, procedures, and processes. The activities and the detailed supporting processes and procedures must be at an adequate level to determine compliance with controls at each applicable system impact level (Low/Moderate/High).

#### Review Documentation

During the planning phase, the Privacy Assessor reviews the ACT Assessment Plan to understand the scope of the assessment. Based on the scope, privacy policies and procedures are reviewed in accordance with <Organization> privacy requirements. In preparation for the assessment phase, the Privacy Assessor will review provided documentation to increase familiarity with the target system. The Privacy Assessor will identify any requests to be made to ensure that the assessment period runs smoothly. During this time, any special requests are provided to the ACT Security Assessment Lead or Risk Assessment Lead for coordination with the system’s Point of Contact (POC) and any applicable <Organization> representatives (*e.g.,* Privacy SME, ISSO).

To prepare for an assessment, the Privacy Assessor reviews provided documentation. Available documentation may include but is not limited to the following (which should be requested):

* System Security Plan (SSP) Privacy Controls
* Privacy Impact Assessment (PIA)
* Information Security Risk Assessment (ISRA)
* Plan of Action and Milestones (POA&M)
* Policy/Procedure/Process documents, such as:
  + Privacy Governance
  + System Privacy Policy
  + Privacy Notice
  + Data Ingest
  + Inventory of PII
  + Privacy Breach Notification Procedures
  + Data Retention and Destruction Policy
  + Privacy Monitoring and Audit Procedures
* Privacy Awareness Training records
* Rules of Behavior (RoB)

#### Conduct Privacy Interview

The system stakeholders (*e.g.,* Privacy SME, ISSO) should provide an overview of their privacy roles and responsibilities related to implementation of the Privacy Program, as well as the privacy controls in place to secure it. The overview should include all components for which they have a specific responsibility to ensure privacy in relation to the application or system. Interview guidance can be found in the Questionnaire-Privacy document (see Section 3 *Attachments*).

#### Consult with Other Assessors

The ACT Assessment Team performs as an integrated and cohesive team. Findings identified in respective assessment areas, such as Network, Operating System, Application, and M&O, often overlap (*e.g.,* The PIA may confirm weak or non-existent privacy processes/procedures/policies). These findings are shared within the team at least daily in preparation for the daily out-brief stakeholder meeting, but it is encouraged that findings and information are shared more often. This serves many purposes: to inform other Assessors, to confirm identified vulnerabilities are not false positives, and helps ensure the Assessors function as a team.

#### Document Findings

Privacy findings focus on the deficiencies discovered in the privacy artifacts the Privacy ACT team member is responsible for assessing as well as those elicited in interviews with system personnel. These include, primarily, the SSP and PIA, and any system privacy processes, procedures, and policies that are missing or need to be enhanced.

All findings in their respective assessment areas are documented by the ACT team to ensure tracking and eventual closure by the system staff. Findings are presented during the daily out-brief call and are typically confirmed with system personnel prior to the call. These findings are considered *draft* findings until confirmed. If a High or Critical severity finding is discovered by the Assessment Team, the Security Assessment Lead will immediately notify the CRA and arrange for a meeting with the appropriate stakeholders, typically the CRA, BO, and system personnel, responsible for the affected system component or process. If it is later determined that a finding is a false positive, it will remain as reported and documented as such.

## Phase 3: Reporting

The **Reporting** phase refers to the documenting of the Security Assessment or Risk Assessment activities, what was assessed, what was not assessed, and the result of the assessment. Reporting concludes with updated versions of the Security Assessment Report (SAR) and/or Risk Assessment Report (RAR) and the finalized version of the Findings and Risks files.

All artifacts generated or collected by the Assessment Team during the assessment are collected and delivered to <Organization> in a Final Package.

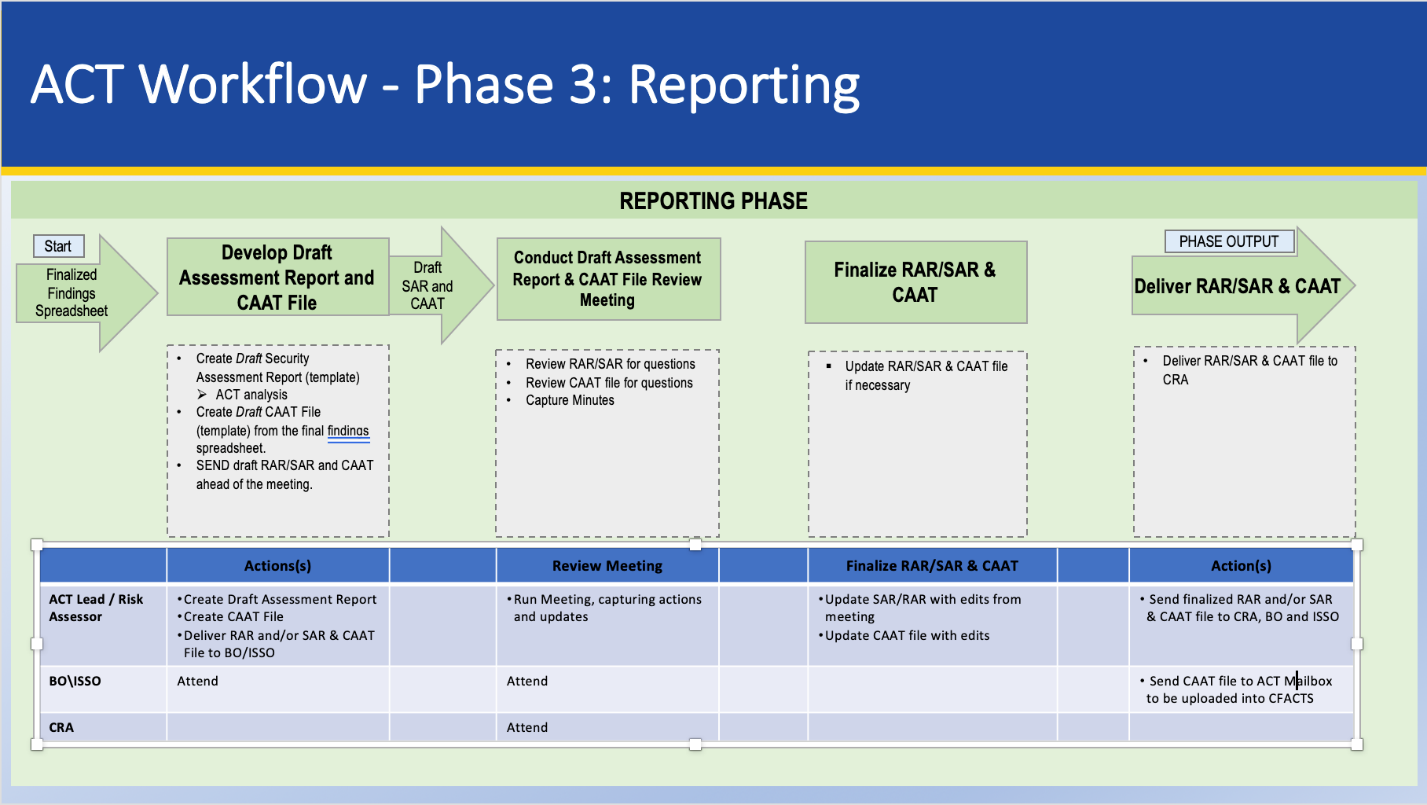


Figure . Phase 3: Reporting

### Develop Assessment Report, Findings File, and Risks File

The Assessment Report provides a summary of the intent, execution, and results of the entire assessment. A Security Assessment Report (SAR) focuses on technical compliance issues (Findings), while a Risk Assessment Report (RAR) focuses on higher-level risks; both report types document recommendations, scope of the assessment, untested portions, and methods used to test. The Security Assessment Lead or Risk Assessment Lead will utilize the ACT Security or Risk Assessment Report Template to create the applicable Assessment Report in preparation for the Assessment Report Review Meeting (see Section 3 *Attachments*). The ACT Findings file and ACT Risks file are specially formatted files that are produced alongside a SAR or a RAR; they are designed to be ingested by automated tracking systems and contain the identified Findings and Risks in well-defined and structured formats. These items need to be sent to all stakeholders, including the ISSO, CRA, and Business Owner prior to the Assessment Review meeting. Low, Moderate, and High Findings and Risks File Templates are provided in Section 3 *Attachments*. **The Assessment Report that is submitted for review at the Assessment Report Review Meeting must be essentially complete and ready for formal publication.**

A sample SAR and RAR are provided in Section 3 *Attachments*, demonstrating best practices for producing these reports.

Inputs and Outputs for this section are:

* Inputs
  + Risk Information Sources (responsible role: Risk Assessment Lead)
    - ACT Security Assessment Report
    - Other Risk Information Source data
  + Consolidated Assessment Findings Spreadsheet (responsible role: Security Assessment Lead)
* Outputs
  + An Assessment Report (select 1)
    - Security Assessment Report (responsible role: Security Assessment Lead)
    - Risk Assessment Report (responsible role: Risk Assessment Lead)
  + A Findings or Risks File (select 1)
    - Findings File (responsible role: Security Assessment Lead)
    - Risks File (responsible role: Risk Assessment Lead)

### Conduct Assessment Report Review Meeting

For both Security Assessments and Risk Assessments, an Assessment Report Review Meeting is conducted with the System Stakeholders, all System POCs, and the Security Assessment Lead or Risk Assessment Lead. This meeting provides an opportunity for all parties to ask any final questions, seek clarification regarding the report findings, ensure that the status of the findings appropriately reflects submitted remediation evidence and (for any reassigned findings) for the receiving party to accept responsibility. The Security Assessment Lead or Risk Assessment Lead can provide clarification for the narrative portion of the Report and for findings transferred from the spreadsheet to the Report.

When a Security Assessment and a Risk Assessment are performed simultaneously for a system, this meeting will typically cover both Reports.

Inputs and Outputs for this section are:

* Inputs
  + Assessment Report (select 1)
    - Security Assessment Report (responsible role: Security Assessment Lead)
    - Risk Assessment Report (responsible role: Risk Assessment Lead)
  + Findings or Risks File (select 1)
    - Findings File (responsible role: Security Assessment Lead)
    - Risks File (responsible role: Risk Assessment Lead)
  + Meeting Notes (responsible role: Security Assessment Lead or Risk Assessment Lead)
* Outputs
  + An Assessment Report (select 1)
    - Security Assessment Report updates (responsible role: Security Assessment Lead)
    - Risk Assessment Report updates (responsible role: Risk Assessment Lead)
  + A Findings or Risks File (select 1)
    - Findings File (responsible role: Security Assessment Lead)
    - Risks File (responsible role: Risk Assessment Lead)
  + Meeting Notes with Action Items (responsible role: Security Assessment Lead or Risk Assessment Lead)

### Update Assessment Report, Findings File, and Risks File

Based on discussions in the Assessment Report Review Meeting, the Assessment Report (SAR and/or RAR), and/or Findings and Risks files are updated and sent to the technical writers to review updates and generate the final (and 508-compliant) versions.

* Inputs
  + Meeting Minutes and Action Items from the Assessment Report Review Meeting (responsible role: Security Assessment Lead or Risk Assessment Lead)
  + Assessment Report Updates (responsible role: Security Assessment Lead or Risk Assessment Lead)
* Outputs
  + Updated Assessment Report (responsible role: Security Assessment Lead or Risk Assessment Lead)
  + An Updated Findings or Risks File (select 1)
    - Updated Findings File (responsible role: Security Assessment Lead)
    - Updated Risks File (responsible role: Risk Assessment Lead)

### Upload Assessment Report, Findings File, and Risks File to <Storage Location>

After they are edited and made 508-compliant by the technical writers, the Security Assessment Lead or Risk Assessment Lead uploads the Assessment Report and Findings and Risks files to <Storage Location>, and then sends an email to all system stakeholders and the <Authorizing Official> informing them of the upload.

### Create and Deliver Final Package

At the conclusion of the Security Assessment or Risk Assessment, the Security Assessment Lead or Risk Assessment Lead creates and provides to <Organization> the Final Package: an archive of all artifacts related to the assessment. The Final Package includes (at minimum):

* Assessment Plans (original and updated (if applicable)) (both Microsoft Word and .pdf formats)
* Assessment Reports (original and updated (if applicable)) (both Microsoft Word and .pdf formats)
* Findings and Risks files (original and updated (if applicable)) (both Microsoft Excel and .pdf formats)
* Security Document Evaluations (both Microsoft Word and .pdf formats) (for Security Assessments)
* All working papers and other artifacts: test plans, test scripts, scan results, packet captures, Meeting Notes, relevant emails, other communications, etc.

Inputs and Outputs for this section are:

* Inputs
  + All Assessment Artifacts (responsible role: Security Assessment Lead or Risk Assessment Lead)
* Outputs
  + Final Package (responsible role: Security Assessment Lead or Risk Assessment Lead)

#### Organization of Final Package

Each Final Package shall be organized using at least the following folder/directory structure and names:

* <SYSTEMNAME> <ASSESSMENT\_KICKOFF\_DATE\_YYYYMMDD>
  + 01 Miscellaneous
  + 02 Preliminary Discussion
  + 03 Assessment Plans
  + 04 System-Provided Artifacts
  + 05 Readiness Review
  + 06 Assessment Period
    - 01 Kickoff
    - 02 Daily Briefings & Findings
    - 03 Assessors
      * Application
        + 01 Data Collection Requests & Tools
        + 02 Assessment Tools and Work Aids
        + 03 Interviews
        + 04 Assessment Artifacts
        + 05 Miscellaneous
      * Cloud
        + 01 Data Collection Requests & Tools
        + 02 Assessment Tools and Work Aids
        + 03 Interviews
        + 04 Assessment Artifacts
        + 05 Miscellaneous
      * Database
        + 01 Data Collection Requests & Tools

DB2 RACF

MySQL

Oracle

PostgreSQL

SQL Server

* + - * + 02 Assessment Tools and Work Aids
        + 03 Interviews
        + 04 Assessment Artifacts
        + 05 Miscellaneous
      * M&O
        + 01 Data Collection Requests & Tools
        + 02 Assessment Tools and Work Aids
        + 03 Interviews
        + 04 Assessment Artifacts
        + 05 Miscellaneous
        + 06 Document Evaluations
      * Mainframe
        + 01 Data Collection Requests & Tools
        + 02 Assessment Tools and Work Aids
        + 03 Interviews
        + 04 Assessment Artifacts
        + 05 Miscellaneous
      * Network
        + 01 Data Collection Requests & Tools
        + 02 Assessment Tools and Work Aids
        + 03 Interviews
        + 04 Assessment Artifacts
        + 05 Miscellaneous
      * Operating System
        + 01 Data Collection Requests & Tools
        + 02 Assessment Tools and Work Aids
        + 03 Interviews
        + 04 Assessment Artifacts
        + 05 Miscellaneous
      * Privacy
        + 01 Data Collection Requests & Tools
        + 02 Assessment Tools and Work Aids
        + 03 Interviews
        + 04 Assessment Artifacts
        + 05 Miscellaneous
      * Risk
        + 01 Data Collection Requests & Tools
        + 02 Assessment Tools and Work Aids
        + 03 Interviews
        + 04 Assessment Artifacts
        + 05 Miscellaneous
      * Virtualization
        + 01 Data Collection Requests & Tools
        + 02 Assessment Tools and Work Aids
        + 03 Interviews
        + 04 Assessment Artifacts
        + 05 Miscellaneous
  + 07 Reports and Findings

Other folders/directories should be created as appropriate, and non-applicable folders (such as “Linux” for a system that runs exclusively on Windows, or “MySQL” for a system that uses only Oracle) should be omitted.

#### Delivery of Final Package

The Security Assessment Lead or Risk Assessment Lead delivers the Final Package by bundling everything into a .zip file of reasonable size (or split across multiple .zip files, if appropriate) and uploading it to the <Storage Location>, or physically on CD or DVD if file size makes upload to or storage in <Storage Location> impractical.

The filename(s) for the Final Package should use the following format:

* <SYSTEMNAME> ACT <ASSESSMENT TYPE(S)> Final Package <YYYYMMDD>

The Security Assessment Lead or Risk Assessment Lead then sends an email to the GTL informing them of Final Package delivery and requesting confirmation of receipt.

## Process Improvement Follow-Up

At the conclusion of every Security Assessment or Risk Assessment, the Security Assessment Lead or Risk Assessment Lead shall follow the then-current <Organization Information Security Group>-defined process for soliciting, documenting, and following-up on Lessons Learned from the Assessment. Consult the GTL for details.

# Attachments

The following attachments are referenced in this Handbook. The Assessor should always use the most current published version of each unless otherwise instructed by the <Organization> CRA or GTL.

Table . Attachments

|  |  |
| --- | --- |
| ID | Name |
| *00* | *ACT Assessment Handbook (this document)* |
| 01 | ACT 2.0 Capabilities and Controls Matrix |
| 02 | Template - Preliminary Intake Form |
| 03 | Authorization Boundary Diagram Guidance |
| 04 | ACT Levels of Testing Rigor Definition |
| 05 | Template - ACT Preliminary Discussion Presentation |
| 06 | Template - Preliminary Discussion Meeting Notes |
| 07 | Template - Security Assessment Plan |
| 08 | Template - Risk Assessment Plan |
| 09 | Template - Readiness Review Presentation |
| 10 | Template - Assessment Kick-Off Presentation |
| 11 | Template - Generic Meeting Notes |
| 12 | Template - Daily Findings |
| 13 | Template - Daily Briefing Agenda |
| 14 | Testing Guide - Web Application Testing |
| 15 | Checklist - Facilities <Organization’s Controls Catalog> Compliance |
| 16 | Questionnaire - Management and Operations |
| 17 | Questionnaire - Privacy |
| 18 | Questionnaire - Application Developer |
| 19 | Questionnaire - Database Administrator |
| 20 | Questionnaire - Network and Operating System |
| 21 | Questionnaire - Mainframe |
| 22 | Template - SSP Evaluation |
| 23 | Template - ISRA Evaluation |
| 24 | Template - CP Evaluation |
| 25 | Template - Security Assessment Report |
| 26 | Template - Risk Assessment Report |
| 27 | Templates - Findings and Risks Files |
| 28 | Final Package Folder Structure |
| 29 | Sample Security Assessment Plan (SAP) |
| 30 | Sample Risk Assessment Plan (RAP) |
| 31 | Sample Security Assessment Report (SAR) |
| 32 | Sample Risk Assessment Report (RAR) |
| 33 | <Organization> Core Controls Selection Methodology |
| 34 | ACT Deliverable Review Panel (DRP) Review Process |
| 35 | ACT Assessment Level of Effort Estimation Tool |

# Acronyms

|  |  |
| --- | --- |
| Acronym | Definition |
| **AC** | Access Control |
| **ACT** | Adaptive Capabilities Testing |
| **AES** | Advanced Encryption Standard |
| **ATO** | Authorization to Operate |
| **ATT&CK** | Adversary Tactics, Techniques, and Common Knowledge |
| **BIA** | Business Impact Analysis |
| **BO** | Business Owner |
| **CCB** | Change Control Board |
| **CCE** | Common Configuration Enumerations |
| **CDM** | Continuous Diagnostics and Mitigation |
| **CIO** | Chief Information Officer |
| **CISO** | Chief Information System Officer |
| **CM** | Configuration Management |
| **COOP** | Continuity of Operations |
| **CP** | Contingency Plan |
| **CRA** | Cyber Risk Advisor |
| **CSIRC** | Computer Security Incident Response Center |
| **CSP** | Cloud Service Provider |
| **CVE** | Common Vulnerabilities and Exposures |
| **CVSS** | Common Vulnerability Scoring System |
| **DHS** | Department of Homeland Security |
| **DISA** | Defense Information Systems Agency |
| **DR** | Disaster Recovery |
| **EUA** | Enterprise User Administration |
| **FedRAMP** | Federal Risk and Authorization Management Program |
| **FFRDC** | Federally Funded Research and Development Center |
| **FIPS** | Federal Information Processing Standards |
| **FISMA** | Federal Information Security Modernization Act |
| **GSS** | General Support System |
| **GTL** | Government Task Lead |
| **HVA** | High Value Asset |
| **I&A** | Identification and Authentication |
| **ID** | Identification |
| **IDS** | Intrusion Detection System |
| **IPS** | Intrusion Prevention System |
| **IR** | Incident Response |
| **ISA** | Interconnection Sharing Agreement |
| **ISCM** | Information Security Continuous Monitoring |
| **ISRA** | Information System Risk Assessment |
| **ISSO** | Information System Security Officer |
| **IT** | Information Technology |
| **M&O** | Management and Operations |
| **MFA** | Multi Factor Authentication |
| **MOU** | Memorandum of Understanding |
| **NIST** | National Institute of Standards and Technology |
| **NISTIR** | NIST Interagency Report |
| **OWASP** | Open Web Application Security Project |
| **PHI** | Protected Health Information |
| **PIA** | Privacy Impact Assessment |
| **PII** | Personally Identifiable Information |
| **POA&M** | Plan of Action and Milestones |
| **POC** | Point of Contact |
| **RA** | Risk Assessment |
| **RACF** | Resource Access Control Facility |
| **RAR** | Risk Assessment Report |
| **RIS** | Risk Information Source |
| **RMF** | Risk Management Framework |
| **RoB** | Rules of Behavior |
| **RPO** | Recovery Point Objective |
| **RTO** | Recovery Time Objective |
| **RVA** | Risk and Vulnerability Assessment |
| **SA&A** | Security Assessment and Authorization |
| **SAR** | Security Assessment Report |
| **SCA** | Security Controls Assessment |
| **SIEM** | Security Information and Event Management |
| **SLA** | Service Level Agreement |
| **SORN** | System of Records Notice |
| **SP** | Special Publication |
| **SSP** | System Security Plan |
| **STIG** | Security Technical Implementation Guide |
| **TLS** | Transport Layer Security |
| **TRB** | Technical Review Board |

**[](https://www.mitre.org/our-impact/mitre-labs/cyber-solutions-innovation-center)**

[**https://www.mitre.org/our-impact/mitre-labs/cyber-solutions-innovation-center**](https://www.mitre.org/our-impact/mitre-labs/cyber-solutions-innovation-center)

1. ACT™ is developed and maintained by [the MITRE Corporation](https://act.mitre.org/). [↑](#footnote-ref-2)
2. Office of Management and Budget (OMB) Circular A-130 defines ATO as follows: “*the official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems.*” [↑](#footnote-ref-3)
3. ACT Security Assessment involves what is commonly referred to as “Vulnerability Assessment” but does not involve what is commonly referred to as “Penetration Testing” (see “Penetration Testing” RIS). [↑](#footnote-ref-4)
4. The ISRA is a document that is typically assessed as part of the ACT Security Assessment. [↑](#footnote-ref-5)
5. POA&M: Plan of Action and Milestones [↑](#footnote-ref-6)
6. For purposes of this Handbook, Penetration Testing is assumed to be *performed* by non-ACT assessors outside of the scope of the ACT Security Assessment or ACT Risk Assessment, and *reviewed and analyzed* by the ACT Assessors as one of the RIS in the ACT Risk Assessment. [↑](#footnote-ref-7)
7. <https://www.cisa.gov/publication/high-value-asset-control-overlay> [↑](#footnote-ref-8)
8. To be considered *“*independent,” the Assessment Contractor, its Assessment Team members, and any contracted third-party individual(s) or organization(s) shall not have a vested interest in the development, maintenance, operation, or documentation of the system to be tested, and shall be free from any actual and reasonably perceived Conflicts of Interest (COI) related to the performance of this work. [↑](#footnote-ref-9)
9. PMP: Project Management Professional [↑](#footnote-ref-10)
10. CISSP: Certified Information System Security Professional [↑](#footnote-ref-11)
11. CISA: Certified Information Security Auditor [↑](#footnote-ref-12)
12. CISM: Certified Information Security Manager [↑](#footnote-ref-13)
13. SANS: SysAdmin, Audit, Network, and Security [↑](#footnote-ref-14)
14. GSNA: GIAC (Global Information Assurance Certification) Systems and Network Auditor [↑](#footnote-ref-15)
15. <https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final> (December 2020). [↑](#footnote-ref-16)
16. <https://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf> (March 2006). [↑](#footnote-ref-17)
17. Link to <Organization> Controls Catalog [↑](#footnote-ref-18)
18. Link to <Organization> IS2P2-type document or other document [↑](#footnote-ref-19)
19. Link to <Organization> TRA-type document or other document [↑](#footnote-ref-20)
20. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf> [↑](#footnote-ref-21)
21. NIST: National Institute of Standards and Technology [↑](#footnote-ref-22)
22. NIST Special Publication 800-37 Revision 2 states “*Historically, NIST has used the terms Authorization Boundary, System Boundary, and Accreditation Boundary interchangeably. In the interest of clarity, accuracy, and use of standardized terminology, the term Authorization Boundary is now used exclusively by NIST to refer to the set of system elements comprising the system to be authorized for operation or authorized for use by an Authorizing Official (i.e., the scope of the authorization).”* [↑](#footnote-ref-23)
23. <https://csrc.nist.gov/glossary/term/Security_Authorization_Boundary> [↑](#footnote-ref-24)
24. This example diagram relates to the Example Test System (TST) Adaptive Capabilities Testing (ACT) Security Assessment Report which can be found at [<Link](https://share.cms.gov/Office/OIT/ISPG/ACT/SitePages/LandingPage.aspx) to TST SAR file>.TST is a fake system that is used to demonstrate various ACT principles and concepts - it does not exist in the real-world. All content is fake and is for educational and demonstration purposes only, although it is written as if the system is real. [↑](#footnote-ref-25)
25. <https://csrc.nist.gov/glossary/term/Assessment_Boundary> [↑](#footnote-ref-26)
26. This example diagram relates to the Example Test System (TST) mentioned previously. [↑](#footnote-ref-27)
27. <https://www.opm.gov/information-management/privacy-policy/privacy-references/sornguide.pdf> [↑](#footnote-ref-28)