

Version <X.Y>

<Date>

Prepared for:

<Organization>

Prepared by:

<Author(s)>

Contract: <Contract ID>

<Other Front Matter>

<Organization-specific legal boilerplate, if applicable>

For Internal <Organization> Use. This document was prepared for authorized distribution only. It has not been approved for public release.



This document is derived from  
*MITRE Adaptive Capabilities Testing (ACT)™*.  
act.mitre.org | act@mitre.org

<Organization>

MITRE Adaptive Capabilities Testing (ACT)™

<System Name> (<System Acronym>)

Information System  
Risk Assessment (ISRA)  
Document Evaluation Checklist

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. |

Purpose

This Information System Risk Assessment (ISRA) Document Evaluation Checklist is designed to help assess the completeness of the application’s ISRA. **The ISRA is a risk assessment document that is maintained and continually updated by the system team.** The evaluation criteria were derived from industry best practices and from <Organization>’s policies and procedures.

How the Checklist Is Used:

1. The document is reviewed to verify that each of the requirements noted in the checklist is adequately addressed in the document.
2. The Status column indicates whether each requirement is:
   1. **Met** **-** The requirement has been completely satisfied, and no additional information needs to be documented.
   2. **Partial -** The requirement has been partially satisfied but there is still missing information as explained in the **Comments** column.
   3. **Not Met -** The requirement has not been satisfied and any additional information noting the reasons are provided in the **Comments** column.
   4. **N/A -** The requirement is not applicable to the system that is being evaluated and the reason that it is not applicable is provided in the **Comments** column.
3. The Comments column contains an explanation if a control is not met, partially met, or not applicable.

**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.

Topics Quick Reference

[1. Evaluation Logistics 1](#_Toc199517926)

[2. Information System Risk Assessment Requirements 1](#_Toc199517927)

[3. Additional Comments 6](#_Toc199517928)

# 

# Evaluation Logistics

Table . Evaluation Logistics

|  |  |
| --- | --- |
| Official System Name | Official System Name |
| System Acronym | ABCD |
| Document Name |  |
| Document Version / Date |  |
| Assessment Date(s) | Jan 1 – 3, 2025 |

Table . Evaluator(s)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Role | Name | Organization | Phone Number | Email Address |
| M&O Assessor |  | Assessment Team |  |  |

# Information System Risk Assessment Requirements

Table . Information System Risk Assessment Requirements

|  |  |  |  |
| --- | --- | --- | --- |
| Index | Assessment Check | Status  (Met, Partial, Not Met, or N/A) | Comments |
|  | Was the ISRA methodology as specified in <Reference Document> followed? |  |  |
|  | Is the RA’s classification or sensitivity clearly marked? |  |  |
|  | Does the RA have a Review Log and has it been maintained? |  |  |
|  | Has the system name, acronym, SOR No., FMIB No. been provided (if applicable)? |  |  |
|  | Has the system been categorized as a General Support System (GSS), GSS sub-system, MA or MA individual application? See below:   * GSS example: Primary network * GSS sub-system examples: Mainframe, Enterprise User Interface, etc. * MA examples: Human Resources Management System, Administrative Finance System, etc. * MA individual application example: Specific function within the MA |  |  |
|  | Has the name of the organization responsible for the system, to include the name of the organization, the address and contract number and name been provided? |  |  |
|  | Has the name of the external organization responsible for the system (if applicable), been provided and included:   * Organization Name * Address * Contract number * Contractor contact information |  |  |
|  | Has the person(s) designated to be the point(s) of contact of the system including business owner, System Developer/Maintainer, SSP Author, and contractor contact information (if applicable) been provided? Information to be provided for each:   * Title * Organization * Address * Mail stop * City, State, Zip * E-mail * Telephone * Contractor contact information |  |  |
|  | Are the security contacts listed and do they include: Two (2) different security contacts - one (1) primary security contact and one (1) different emergency contact responsible for the security of the system and the Component ISSO? Information to be provided for each:   * Title * Organization * Address * Mail stop * City, State, Zip * E-mail * Telephone * Contractor contact information (if applicable) |  |  |
|  | Has the operational status been identified as New, Operational, or Undergoing a Major Modification? |  |  |
|  | Has a description of the business process supported by the system been provided? It should include:   * Location of the system: street address and information pertaining to the system location * Business functions description * Underlying business processes and resources including inputs, processing, functions, organizational/personnel roles and responsibilities, and expected outputs/products * Information flows or processed by the system * Internal or external organizations that comprise the user community * Users’ level of access to system-related data, system-related facilities, and IT resources * If GSS, all applications supported by the GSS, if an MA, unique name/identifiers and functions |  |  |
|  | Has a description of the operational/system environment and any special considerations been provided? This includes:   * Communications requirements * User-interface expectations * Network connectivity requirements |  |  |
|  | Does the system description include:   * General description of the technical aspects * Use of PDAs or wireless technology * Network connectivity diagram illustrating system components and security devices |  |  |
|  | Does the system environment description include:   * Purpose of the system * Capabilities of the system * Functional requirements * System environment * Owned or leased * Government, contractor, or privately operated * Hours of operation * Total number of users and user types * Critical processing periods * External organizations and users * Applications supported by system and the functions * System access methods * Information data and data stores and corresponding security controls |  |  |
|  | Is the architecture and topology information provided, or if included in another plan is the name of the plan provided? |  |  |
|  | Is a detailed description of the system boundaries and technical components provided? |  |  |
|  | Is a detailed description of the primary platforms and systems components including server names, vendors, version and security software protecting the system and information provided? |  |  |
|  | Are all interconnectivity interfaces, web portals, distributed and collaborative computing environments included? Information should include:   * Connectivity between system modules * For any system that allows individual web-based access (Internet, Intranet, or Extranet) include: * The URL for the web-based transaction * All authentication products * Electronic logons per year * No. of registered users and their types (internal, contractor, etc.) * Customer groups authenticated |  |  |
|  | Does the RA describe any special security concerns (e.g., Internet connection, etc.)? |  |  |
|  | Does the RA describe system interconnections and information sharing with other systems including Memorandums of Understanding or Agreements (MOU/MOA) for each interface, including the Internet/Intranet and all interfacing systems (if applicable)? |  |  |
|  | Is the system security level provided including all information types? |  |  |
|  | Has the level of authentication needed to access the system been determined? |  |  |
|  | Have business risks and associated safeguards been documented as required by applicable regulations? |  |  |
|  | Have system risks and associated safeguards been documented as required by applicable regulations? |  |  |

# Additional Comments