|  |
| --- |
| Evaluation of the INSERT SYSTEM/APPLICATION NAME HERE Risk Assessment Insert IS RA Date, IS RA Version No. |
| Reference MITRE ACT Assessment Handbook v1.0  INSERT DATE HERE |
| Evaluators Name:  Evaluators Email Address:  Evaluators Telephone Number: |
| **NOTICE**  <Contract Notice goes here as needed> |

|  |
| --- |
| Evaluators Instructions  **IMPORTANT:** **This page must be removed prior to either hardcopy or electronic distribution.**  The instructions are intended to provide guidance to the evaluators for consistency when evaluating RAs for systems.   1. Update all areas highlighted in yellow with the appropriate information. 2. All systems should be reviewed against the most current guidance and templates. 3. If the risk assessment states that a risk acceptance has been granted, all CISO acceptance letters must be requested. These letters are only valid for a year. If they cannot be provided this is a finding. 4. If there are issues, missing information, or a risk that has not been identified repeat index rows 25 and 26 to accommodate all risks that are not documented correctly. Insert as many rows as necessary to correspond with the number of risks identified in the RA which are not complete. In each row replace the ‘System Acronym-99’ with the associated business risk or system item number from the RA. 5. In the comments column note all missing or incomplete information for each risk that is incomplete and any associated comments. 6. General or overall comments and any additional feedback can be added in the Additional Comments section at the end. |

# Risk Assessment Checklist

This Risk Assessment (RA) Evaluation Checklist is designed to help assess the completeness of the system’s risk assessment. The evaluation criteria that make up the checklist were derived from the guidance in the *MITRE ACT Assessment Handbook v1.0*[[1]](#footnote-1).

## How the Checklist Is Used

1. The RA is reviewed to verify that each of the CMS requirements noted in the checklist is included in the RA and analyzed to determine if the information provided adequately addresses the requirement.
2. In the status column, an indication on whether each requirement is:
   * **Met** **-** The requirement has been completely satisfied and no additional information needs to be documented
   * **Partial -** The requirement has been partially satisfied but there is still missing information as explained in the **Comments** column
   * **Not Met -** The requirement has not been satisfied and any additional information noting the reasons are provided in the **Comments** column
   * **N/A -** The requirement is not applicable to the system or application risk assessment that is being evaluated and the reason that it is not applicable is explained in the **Comments** column
3. The comments column contains an explanation if a control is not met, partially met, or not applicable.

| **Index** | Risk Assessment  **Requirement** | **Status**  **Met, Partial, Not Met or N/A** | Comments |
| --- | --- | --- | --- |
|  | Was the IS RA 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? |  |  |
|  | Business Risk Item Number:  *System Acronym-99* |  | 1. Item No. 2. Business Function 3. Risk Level 4. Threat Name 5. Vulnerability Name 6. Risk Description 7. Business Impact 8. Existing Controls 9. Likelihood of Occurrence 10. Impact Severity of Occurrence 11. Risk Level of Occurrence   **For MODERATE and HIGH Risk 12-17 must be completed**   1. Recommended Safeguard Description 2. Residual Likelihood of Occurrence 3. Residual Impact Severity 4. Residual Risk Level 5. Implementation Priority 6. Implementation Rationale |
|  | System Risk Item Number:  S*ystem Acronym-99* |  | 1. Item No. 2. Business Function 3. Risk Level 4. Threat Name 5. Vulnerability Name 6. Risk Description 7. Business Impact 8. Existing Controls 9. Likelihood of Occurrence 10. Impact Severity of Occurrence 11. Risk Level of Occurrence   **For MODERATE and HIGH Risk 12-17 must be completed**   1. Recommended Safeguard Description 2. Residual Likelihood of Occurrence 3. Residual Impact Severity 4. Residual Risk Level 5. Implementation Priority 6. Implementation Rationale |

## Additional Comments

1. Documentation at act.mitre.org [↑](#footnote-ref-1)