|  |  |
| --- | --- |
|  |  |
| Evaluation of the INSERT SYSTEM/APPLICATION NAME HERE Contingency Plan Insert CP Date, CP 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 CPs for systems.

1. Update all areas highlighted in yellow with the appropriate information.
2. For each of the CP requirements, evaluate each of them to determine that the preparer has addressed the compliance of the CP controls as required by <relevant authority or regulation>.
3. Ensure sufficient detail is provided in the CP to provide for recovery of the system/application.
4. General or overall comments and any additional feedback can be added in the *Additional Comments* section at the end.

# Contingency Plan Evaluation Checklist

This Contingency Plan (CP) Evaluation Checklist is designed to help assess the completeness of the application’s CP. The evaluation criteria were derived from the procedures documented in the *MITRE ACT Assessment Handbook v1.0[[1]](#footnote-1)*.

## How the Checklist Is Used

1. The CP is reviewed to verify that each of the requirements noted in the checklist is included in the CP and analyzed to determine if the information provided adequately addresses the requirement.
2. In the status column, an indication on 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 or application CP 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.

| Index | Contingency Plan Requirement | **Status**  **Met, Partial, Not Met or N/A** | Comments |
| --- | --- | --- | --- |
| 1. 1 | The *MITRE ACT Assessment Handbook v1.0* shall be followed. |  |  |
| 1. 3 | The CP’s classification or sensitivity shall be clearly marked. |  |  |
|  | The CP version number and the date shall reflect the most recent version of the CP. The date should reflect the last date a review was recorded in the *Review Log*. |  |  |
|  | The *Review Log* shall contain a record of completed reviews which includes the following information:   * Date of the review * Name of the reviewer * Staff reviewer’s organization * CP version reviewed. |  |  |
|  | The *Review Log* shall cover a three-year time span.  Note: depending on when the new format was adopted the Review Log may not cover three years. |  |  |
|  | All CP support documentation shall be provided in the CP or its appendices or the CP shall reference the name and location of any documentation with support information. |  |  |
|  | The CP shall identify vital records for the application which includes documents required to identify, restore and maintain the application. |  |  |
| 1. 1 | There must be a section that provides a summary of the procedures and associated responsibilities for their execution for notification, activation, recovery and restoration. |  |  |
| 1. 2 | There must be a section that identifies the application and any associated sub-applications with the application acronyms. |  |  |
| 1. 4 | There must be a section that clearly defines the roles and responsibilities for various task assignments and deliverables for the CP process. |  |  |
| 1. 5 | The roles defined in the plan shall include at a minimum the business owner, contingency plan coordinator, system developer/maintainer, and the infrastructure/data center support. |  |  |
|  | There must be a section that documents the issues, situations and conditions addressed and not addressed in the CP. |  |  |
|  | There must be a section that provides the following:   * Application identifier * Application CP version number and release date * Summary of changes * Section numbers and paragraphs modified * Staff that authorized changes |  |  |
| 1. 6 | There must be a section that provides information on the application and the business processes supported by the application and include the general location of all users. |  |  |
|  | The application description shall provide:   * Application/system name * System acronym * System of record designation * Financial Management Investment Board (FMIB) number (if applicable) * Organization name * Address * Contractor name * Contract number * Business owner * Business owner title * Business owner address * Business owner email address * Business owner phone number |  |  |
|  | There must be a section that provides information on any interdependencies both internal and external to the organization including applications, systems, and partnerships with other organizations. |  |  |
|  | There must be a section that provides a description of the technical environment in which the application executes the physical location of the application and the operating environment. |  |  |
|  | There must be a section that identifies and documents all applications or systems that support the application (feeds the application) or that the application supports (the application feeds information to). |  |  |
|  | There must be a section that provides a current diagram of the architecture to include security controls and telecommunication connections. |  |  |
|  | There must be a section that documents interconnection agreements and memorandum of understandings information and includes the name of the system, the organization owning the connecting system, and the type of interconnection. |  |  |
|  | There must be a section that includes the business owner and system developer/maintainer checklist with a complete list of contingency steps. |  |  |
|  | The notification/activation checklist shall address activities for all disaster types in the order and within the timeframe in which the activity should occur relative to the reporting of the incident or event. |  |  |
|  | The CP shall clearly specify the determination criteria for disaster. |  |  |
|  | There must be a section that specifies the personnel responsible for assessing damage. |  |  |
|  | There must be a section that provides a line of succession by role that specifies who should assume responsibility in the absence or unavailability of the business owner. The contact information for the line of succession must be included. |  |  |
|  | There must be a section that specifies key roles with any responsibilities associated with the application. The contact information for the key roles must be included. |  |  |
|  | There must be a section that includes documented recovery functions for temporary manual processing (if applicable), recovery and operations on an alternate system (if applicable), and/or relocation and recovery at an alternate site. |  |  |
|  | There must be a section that specifies recovery teams to which includes:   * Team name * Names and titles of team members * Onsite and offsite contact information * Roles and responsibilities of all team members |  |  |
|  | The application recovery priority shall be specified and include all application sub-components necessary for the application to function, the recovery priority of each, and the associated hardware and associated software. |  |  |
|  | Recovery prerequisites shall be specified for all disaster recovery types and scenarios and include required jobs to be executed and data that must be available. |  |  |
|  | The CP shall specify the alternate storage site, the alternate processing site and the telecommunications services used during the recovery, the organizations responsible, and the CP or other documentation that addresses that information. |  |  |
|  | The CP shall specify the regular backup processes and any application unique backup and recovery/restoration procedures. This includes information on any agreement by the data center to perform additional backup procedures outside of the routinely performed backup processes. |  |  |
|  | The recovery and restoration procedures shall include both technical and business services procedures related to the application to support recovery of that application. |  |  |
|  | The recovery and restoration procedures shall be documented in a checklist format and include the following information:   * Application business owner or designated alternate(s) * Date of incident * Time of incident * Type of incident * Description of incident * Facility/application or business impacted * Expected duration * Completion status * Detailed recovery and restoration procedures based on type of incident |  |  |
|  | The organizations and roles responsible for returning the application to normal operations shall be documented. |  |  |
|  | The return to normal operations procedures shall include a step that specifies the testing of the application according to the CP testing procedures. |  |  |
|  | The CP shall specify the method to clear the application and any application specific information or data from the recovery site. The steps shall address the handling of sensitive information. |  |  |
|  | The CP shall include procedures for packing, labeling, and shipping all materials, equipment and backup media from the alternate site to the appropriate locations associated with the restored or new permanent site. |  |  |
|  | There must be a section that includes the name, office, home and cell phone numbers and email address for all contacts. |  |  |
|  | There must be a section that includes the following for equipment provided by a third-party vendor:   * Vendor name * Vendor contact person * Reference documentation listing * Phone number of vendor contact * Email address of vendor contact |  |  |
|  | There must be a section that documents component/group; contact person; area of responsibility; version of the software; version of the hardware; and reference documentation. |  |  |
|  | There must be a section that includes all applicable service agreements. |  |  |
|  | There must be a section that includes the following information:   * Cause of the disruption or disaster * Potential for additional disruption or damage * Area affected * Status of the infrastructure (as applicable) * Inventory and functional status of IT equipment (e.g., fully functional, partially functional, and non-functional) * Type of damage to IT equipment or data (e.g., water, fire and heat, physical, or electrical surge) * Items to be replaced (e.g., hardware, software, firmware, and supporting materials) * Estimated time to restore normal services. |  |  |
|  | There must be a section that provides documentation information which includes:   * Document name * Date and/or version number * Media * Department * Contact |  |  |
|  | There must be a section that includes a connectivity diagram or data flow diagram, inter-dependencies/interfaces, and a current configuration table. |  |  |
|  | There must be a section that includes the most current copy of the business owner’s signed certification document. The business owner CP certification shall include a statement certifying that the business owner has reviewed the CP recovery procedures, that the procedures are accurate and complete, that the CP has been tested and that all parties know and accept their roles. |  |  |

## Additional Comments

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