

**Department of the Army  
Pamphlet 25-1-2**

**Information Management**

# **Information Technology Contingency Planning**

**Headquarters  
Department of the Army  
Washington, DC  
10 August 2020**

**UNCLASSIFIED**

# ***SUMMARY of CHANGE***

DA PAM 25–1–2

Information Technology Contingency Planning

This administrative revision, dated 1 November 2022—

- o Changes proponency from CIO/G–6 to Deputy Chief of Staff, G–6 (title page).

This major revision, dated 10 August 2020—

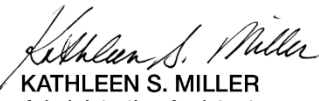
- o Clarifies the relationship between contingency planning and continuity of operations planning (para 1–5).
- o Addresses contingency planning for enterprise information systems (throughout).
- o Updates contingency planning guidance to align with AR 25–2, AR 500–3, DOD Senior Information Security Officer memo, “Contingency Planning for DOD Information Systems,” and National Institute of Standards and Technology Special Publication 800–34 (throughout).

## Information Management Information Technology Contingency Planning

By Order of the Secretary of the Army:

**JAMES C. MCCONVILLE**  
*General, United States Army  
Chief of Staff*

Official:

  
**KATHLEEN S. MILLER**  
*Administrative Assistant  
to the Secretary of the Army*

**History.** This publication is an administrative revision. The portions affected by this administrative revision are listed in the summary of change.

**Summary.** This pamphlet provides operational procedures, practical guidance for information technology contingency

planning, and the development of information system contingency plans.

**Applicability.** This pamphlet applies to the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated. It applies to all Army information technology, operational technology, and information in electronic format.

**Proponent and exception authority.** The proponent for this pamphlet is the Deputy Chief of Staff, G–6. The proponent has the authority to approve exceptions or waivers to this pamphlet that are consistent with controlling law regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this pamphlet by providing

justification that includes a full analysis of and the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the respective policy proponent. Refer to AR 25–30 for specific guidance.

**Suggested improvements.** Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) via email to [usarmy.pentagon.hqda-dcs-g-6.mbx.publications-management@army.mil](mailto:usarmy.pentagon.hqda-dcs-g-6.mbx.publications-management@army.mil).

**Distribution.** This pamphlet is available in electronic media only and is intended for the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

### Contents (Listed by paragraph and page number)

#### Chapter 1

##### Introduction, page 1

Purpose • 1–1, page 1

References and forms • 1–2, page 1

Explanation of abbreviations and terms • 1–3, page 1

Exceptions • 1–4, page 1

Information Technology Contingency Planning support to continuity of operations • 1–5, page 1

#### Chapter 2

##### General Requirements, page 4

General information technology contingency planning requirements • 2–1, page 4

Risk management framework contingency planning security controls • 2–2, page 4

Contingency planning and the system development life cycle • 2–3, page 5

Roles in planning for information technology contingencies • 2–4, page 7

#### Chapter 3

##### Information Technology Contingency Planning Process, page 9

Overview • 3–1, page 9

Develop the contingency planning policy • 3–2, page 9

Conduct a business impact analysis • 3–3, page 10

Identify preventive controls • 3–4, page 11

Create contingency strategies • 3–5, page 11

\*This pamphlet supersedes DA Pam 25-2-1, dated 6 June 2012.

## Contents—Continued

Develop the information system contingency plan • 3–6, *page 14*  
Plan testing, training, and exercises • 3–7, *page 15*  
Information system contingency plan maintenance • 3–8, *page 17*

### Appendixes

A. References, *page 19*

### Table List

Table 3–1: NIST SP 800–34 sample alternate site criteria, *page 13*  
Table 3–2: Recovery strategy budget planning example (in dollars), *page 14*

### Figure List

Figure 1–1: Mission essential function owner/continuity of operations plan writer determined/provided information, *page 2*  
Figure 1–2: Information from Mission Essential Function review to develop an information system contingency plan, *page 3*  
Figure 2–1: System development life cycle, *page 6*

### Glossary

## **Chapter 1**

### **Introduction**

#### **1–1. Purpose**

This pamphlet provides operational procedures, practical guidance for information technology (IT) contingency planning, and the development of information system contingency plans (ISCPs). The requirement for the development of ISCPs includes general support systems, major applications, and platform information technology (PIT). The primary focus of this document is the implementation of procedures mandated by AR 25–1, AR 25–2, AR 500–3, AR 70–1, AR 190–13, AR 190–51, DA Pam 190–51, and Department of Defense Instruction (DoDI) 8500.01. This document follows the guidelines in Department of Defense (DoD) Senior Information Security Officer memorandum, National Institute of Standards and Technology (NIST) Special Publication (SP) 800–34, NIST SP 800–53, and Committee on National Security Systems Instruction (CNSSI) 1253.

#### **1–2. References and forms**

See appendix A.

#### **1–3. Explanation of abbreviations and terms**

See the glossary.

#### **1–4. Exceptions**

This pamphlet only addresses IT contingency planning supporting continuity of operations (COOP). The Army's COOP program is addressed in AR 500–3.

#### **1–5. Information Technology Contingency Planning support to continuity of operations**

*a.* The Army COOP program's mission is to assure the capability to continue an organization's mission essential functions (MEFs) required to be performed within the first 30 days of an event under all circumstances, in accordance with AR 500–3. The MEF review includes an impact analysis of the organization's mission for each MEF not conducted and the maximum tolerable downtime (MTD) the organization can tolerate. ISCPs are developed to ensure that the information systems, applications, and databases are available to meet each organization's MTD. Figure 1–1 shows a generic, notional example of the information that an organization is required to identify during the review. A MEF owner normally identifies the MTD along with the primary/alternate communications, information systems, applications, and databases that support the MEF. This information aids in determining the potential impact to the MEF if supporting resources become unavailable. Impact would be categorized as high, moderate, or limited. The MEF priority would be determined by the organization's commander or director, considering the effect on the organization's mission if the MEF was not performed and the MTD exceeded. Figure 1–2 shows the information from one MEF that is used in developing an ISCP.

*b.* An ISCP is not a COOP plan, but an ISCP is frequently a supporting plan critical to an organization's COOP plan, and performing its MEF. A COOP plan is a set of policies, plans, procedures, and capabilities that addresses the subset of an organization's MEFs that are deemed most critical. A COOP plan, as stated in AR 500–3, enables the sustainment of MEFs within 12 hours of, and for a minimum of 30 days after, a disaster event before returning to normal operations or reconstitution. It is usually written at the headquarters level, is not IT-focused, and cannot be used as a substitute for an ISCP. The ISCP establishes procedures for the assessment and recovery of a system following a system disruption that supports MEFs. The ISCP may be prepared in coordination with COOP planning to the degree that a particular system is necessary to support MEFs.

MEF Owner / Organization COOP Planner	Example Mission Essential Functions (MEF)	Potential Impacts	Max Tolerable Downtime*	MEF Priority	MEF Required Systems, Applications & Databases
	Coordinate Current Operations	Perations - Unit's missions, personnel, Equipment, capabilities	4 Hours	1	Systems, Applications & Databases **
	Monitor & Report Readiness	Readiness - Ability to Support future operations	12 Hours	4	Systems, Applications & Databases **
	Intelligence Support	Intelligence - Impact to current and future operations	6 Hours	3	Systems, Applications & Databases **
	Operate & Secure Networks	User support for staff to timely execute MEF and missions	4 Hours	2	Systems, Applications & Databases **
* Times Notional					

\*\*(1) If a Primary or Alternate System, Application, or database to Perform each MEF, and  
 (2) Impact on Performing the MEF if the System, Applications, or Database is Not Available; High, Moderate, or Limited

## MEF Owner / Organization COOP Planner Determined / Provided Information

Figure 1-1. Mission essential function owner/continuity of operations plan writer determined/provided information

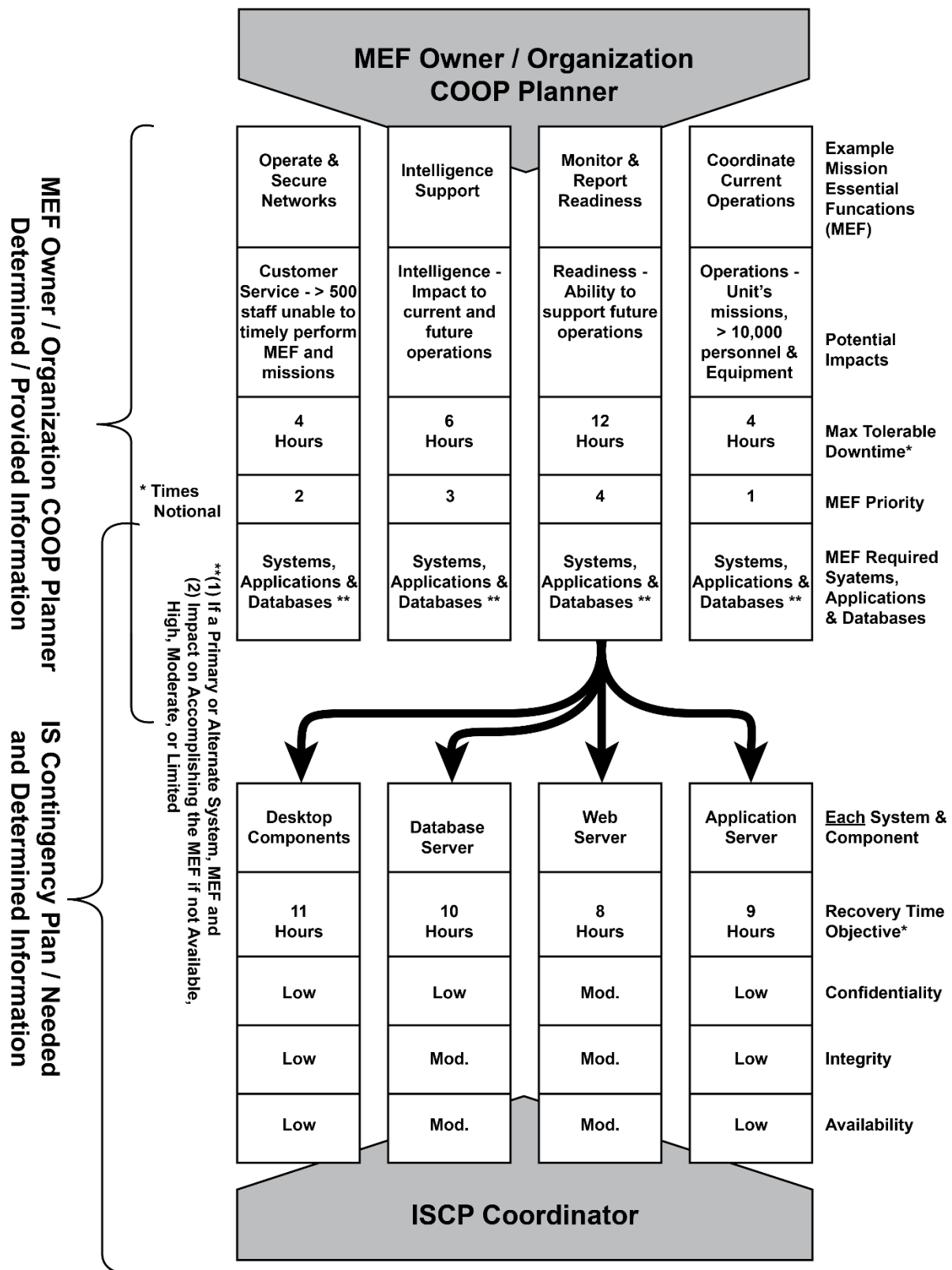


Figure 1-2. Information from Mission Essential Function review to develop an information system contingency plan

## Chapter 2

### General Requirements

In accordance with AR 25–2, every Army PIT system and information system requires a unique ISCP that provides procedures to respond to system capability disruptions.

#### 2–1. General information technology contingency planning requirements

a. IT contingency planning requires a long-term strategy and program management plan. The planning process is to outline how the organization will designate resources, define short and long-term goals and objectives, forecast budgetary requirements, anticipate and address issues and potential obstacles, discuss MEFs, and establish planning milestones. A well-defined IT portfolio management and evaluation methodology is essential for assessing contingency planning as related to the existing baseline enterprise architecture. A lack of understanding of how contingency planning relates to the enterprise architecture will result in a lack of funding and effort needed to implement effective and efficient approaches of crisis restoration across the IT enterprise. In addition, this leads to the inability of the Army to provide and plan for funding, cybersecurity, hardware and software applications, and for staffing during crisis management scenario operations.

b. IT contingency planning should:

- (1) Be addressed throughout the system development life cycle (SDLC) (see para 2–3).
- (2) Establish a primary and an alternate ISCP coordinator with the responsibility for planning and developing the ISCP (see para 2–4).
- (3) Support a command's COOP planning (see para 1–5).
- (4) Address risk management and mitigation (see para 2–2).
- (5) Address business impact for the services the system provides (see para 3–3).
- (6) Establish procedures to restore full system capability (see para 3–5).
- (7) Create a Federally compliant ISCP (see para 3–6).
- (8) Address plan testing, training and reporting (see para 3–7).
- (9) Address how ISCP requirements will be incorporated into daily operations (see para 3–5).
- (10) Address how the ISCP relates to other disaster and emergency plans (see para 1–5).
- (11) Evaluate the system to link these critical services to system resources (see para 3–3).

c. In accordance with AR 25–1, all fielded mission critical (MC), mission essential (ME), and mission support IT systems, as well as all the acquisition category I through III MC/ME IT systems in development, must be recorded in the Army Portfolio Management Solution (APMS). These systems must also be registered with the Army Chief Information Officer (CIO)/G–6 and the DoD CIO in accordance with AR 70–1. Any information system (IS) supporting a command's MEF is by definition an MC/ME IT system. Information on the requirements for survivability of MC/ME systems can be obtained in AR 70–75.

d. To be compliant with Army requirements, information system owners (ISOs) register the system in APMS and ensure a contingency plan is developed and tested at least once a year. This is done more often as necessary to ensure operational readiness, functionality, availability, interoperability, and network connectivity between the system at the alternate site and users at their primary and alternate locations. If the system is fielded to multiple locations, the ISO must coordinate with the system administrators at each location and the system administrators must implement and extend the ISCP as appropriate for that location, whether it is at the organizational level or installation level. After the completion of the test, there are two fields listed below that are mandatory for the ISOs to complete and record in the APMS. For more information regarding APMS refer to DA Pam 25–1–1. Also, see paragraph 2–4c for additional information about system owner responsibilities.

(1) *Contingency plan.* This field indicates if a contingency plan is in place to account for disruptions in the operation of this system. It is a mandatory DoD IT portfolio repository data element for all systems.

(2) *Contingency test date.* This field indicates the last date the ISCP was exercised. It is a mandatory DoD IT portfolio repository data element for all systems with an ISCP.

#### 2–2. Risk management framework contingency planning security controls

a. From the information system contingency planning perspective, the risk management framework (RMF) actively supports the development, implementation, testing, and maintenance of an information system's contingency plan as it supports the mission of the organization. Effective contingency planning includes incorporating security controls early in the development of an information system, and maintaining these controls on an ongoing basis.

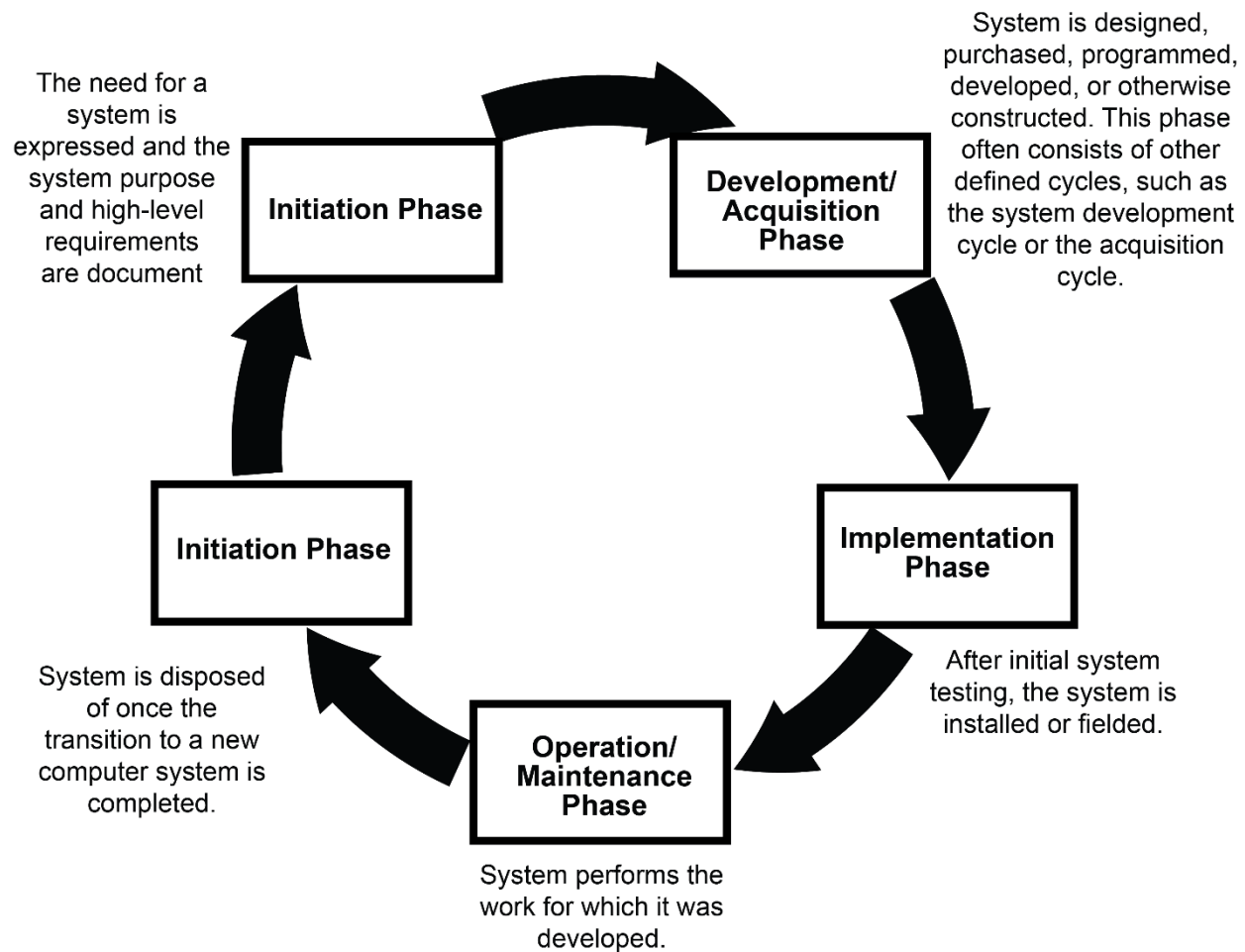
b. NIST SP 800–53 identifies nine contingency planning security controls for information systems. Not all controls are applicable to all systems. The CNSSI 1253 security categorization determines which controls apply to a particular



system. For example, information systems that have availability as a security objective categorized as low-impact do not require alternate processing or storage sites. In contrast, information systems that have an availability security objective categorized as moderate-impact require compliance with only the first system backup control enhancements. Using the CNSSI 1253 security categorization allows for tailoring of the security controls in NIST SP 800–53 to those applicable to the appropriate security control baselines. For further guidance on the Army implementation of the DoD RMF process see DA Pam 25–2–14.

### **2–3. Contingency planning and the system development life cycle**

*a.* The SDLC refers to the full scope of activities conducted by ISOs associated with a system during its life span. IT contingency planning is similar to all Army planning. The process starts with program executive officers (PEOs) and program managers (PMs) and carries on to the system owner and users. The ISCP is an organic document, meaning it can and must change whenever necessary. Although contingency planning is associated with activities occurring mostly in the operation/maintenance phase, identification and integration of contingency and continuity strategies at all phases of the life cycle allow the owner to build layered protection against risks and assist implementation of effective recovery strategies early on in development. This approach reduces overall contingency planning costs, enhances contingency capabilities, and reduces impacts to system operations when the contingency plan is implemented. The SDLC is depicted in figure 2–1.



**Figure 2-1. System development life cycle**

---

*b. Initiation phase.* IT contingency planning should be comprehensive and must receive support and funding at the onset of system development. The failure to address contingency planning requirements early in development will be difficult and costly to overcome as the system progresses through the life cycle.

(1) In this phase, system requirements are identified, matched to their related operational processes, and initial contingency requirements.

(2) During this phase, new IT systems should be evaluated against all other existing and planned IT systems to determine appropriate recovery priority.

(3) The deliverable for this phase would be a general ISCP addressing issues that are not site-specific. Below are the elements this should include:

- (a) Completing data backup procedures.
- (b) Performing disaster and recovery planning.
- (c) Identifying essential system functions.

*c. Development and acquisition phase.* As initial concepts develop into system designs, specific contingency solutions may be incorporated. As in the initiation phase, contingency measures included in this phase should reflect system and operational requirements. In cases where applications and systems are developed by a PM, a standard method for contingency planning should be provided to customers.

(1) The design should incorporate redundancy and robustness directly into the system architecture to optimize reliability, maintainability, and availability during the operation/maintenance phase.

(2) If multiple applications are hosted within the new general support system, individual priorities for those applications should be set to assist with selecting the appropriate contingency measures and sequencing for the recovery execution.

(3) Examples of contingency measures considered in this phase include:

(a) Redundant communication paths.

(b) Single points of failure.

(c) Enhanced fault tolerance of network components and interfaces.

(d) Power management systems with appropriately sized backup power source.

(e) Load balancing.

(f) Data mirroring and replications.

d. *Implementation phase.* As the system undergoes initial testing, contingency strategies also should be tested to ensure technical features and recovery procedures are accurate and effective.

e. *Operation and maintenance phase.* Users, administrators, and managers will maintain a training and awareness program which addresses ISCP procedures in accordance with AR 25–2 and FISMA guidelines.

(1) Exercises and tests should be conducted to ensure procedures remain current and effective.

(2) System backups should be created and stored offsite.

(3) The ISCP should be updated to reflect changes to procedures based on lessons learned through after action reviews conducted at the end of each test or event.

(4) Modifications should be reflected in the ISCP when IT systems are upgraded or modified.

(5) Documented changes should be incorporated in a timely manner to maintain an effective ISCP.

f. *Disposal phase.* Contingency considerations for an existing system remain in effect during transition to a replacement capability.

(1) Until the new system is fully tested, accredited, and operational (including its contingency capabilities), the original ISCP applies. As legacy systems are replaced, they may provide a valuable backup capability if a loss or failure of the new system should occur.

(2) Legacy systems can be used as test systems for new applications, allowing potentially disruptive system flaws to be identified and corrected on non-operational systems.

g. *Additional guidance.* For additional guidance on common ways that contingency strategies can be incorporated throughout the SDLC see NIST SP 800–34.

## **2–4. Roles in planning for information technology contingencies**

a. *Commanders.* IT contingency planning is a command responsibility. Commanders are integral in the establishment of a fully incorporated and authoritative contingency planning program. A commander's lack of attention to planning would bring about a loss of funding or inability to operate. The ISCP policy should clearly designate an ISCP coordinator and at least one alternate with the assigned duties to develop, maintain, and test the ISCP. ISCP testing should be scheduled and conducted prior to funding cycles to ensure proper funding is identified to address plan deficiencies.

b. *Program executive officers and program managers.* PEOs and PMs have the same role as stated in AR 25–1. IT contingency planning is a life cycle development process that is most effective when implemented in the development and configuration management stages. PEOs/PMs provide the initial equipment and identify the system's MC/ME functions along with its baseline capabilities. During the initial phases of system development, PEOs/PMs develop a general ISCP to be provided to receiving system owners and users for further tailoring as the system is fielded in their respective environments. (See paragraph 2–3b(3) for the elements that should be addressed in a general ISCP.)

c. *Information system owner.* The ISO is the government civilian or military person responsible for introduction or operation of any IT used by or in support of the Army. The ISO is responsible for ensuring the security of the IT system as long as it remains in Army inventory, or until transferred (temporarily or permanently) to another government person or organization and such transfer is appropriately documented and provided as an artifact to the authorization package.

d. *Network enterprise center and information system contingency plan coordinators.* Designated by the commander as the primary ISCP point of contact (POC), the ISCP coordinator, who may be located at the NEC, is responsible for overseeing all aspects of contingency planning. However, if another individual is appointed the POC outside the NEC, then he or she may hold authority over the NEC and is then responsible for the ISCPs. Regardless of whether the ISCP coordinator is located within the NEC, the ISCP coordinator has the authority to take independent action

when necessary to maintain operational information systems and oversee all aspects of contingency planning. The ISCP coordinator should—

(1) Operate as the ISCP POC as coordinated and managed under the Army COOP program. Due to operational security concerns, an ISCP alternate processing site should not be used interchangeably with a COOP site. While an ISCP might be executed at a COOP site (or vice versa), it is important to maintain the operational security of COOP sites by not correlating an ISCP location with any COOP location.

(2) With the involvement of functional users and tenants, identify all organizational functions.

(3) Maintain a copy of pertinent installation service agreements and contract numbers with their vital records.

(4) Support or conduct a business impact analysis (BIA) (see para 3–3).

(5) In coordination with the COOP site manager, develop a plan to test the ISCPs. Refer to paragraph 3–7 for guidance on ISCP testing and training.

(6) Coordinate with U.S. Army Cyber Command or other IT support providers as required and engage in quarterly communications exercises with supported tenants and IT support elements.

(7) Maintain a copy of the ISCP for each associated system and a list of those to whom the plan was distributed.

(8) Communicate changes in the ISCP to representatives of associated plans or programs, as necessary, and record plan modifications.

(9) Coordinate frequently with associated internal and external organizations and system POCs to stay aware of necessary changes to the ISCP based on changes to systems and requirements.

(10) Refer to AR 380–5 for information pertaining to the protection of information in an emergency situation.

(11) Evaluate supporting information to ensure the information is current and meets system requirements.

(12) Ensure that only official and approved changes are made to the plan.

(13) Recommend ISCP activation if any activation criterion is met.

(14) Select an appropriate recovery strategy upon activation of the plan.

(15) Determine how often media should be backed up.

(16) Select appropriate disk replication techniques and products.

(17) Assess the robustness and reliability within their core networks.

*e. System users.* System users are those organizations or personnel that utilize any portion of an information system, capability, or application.

*f. Continuity of operations point of contact.* COOP points of contact coordinate results of MEF prioritization and continuity planning with ISCP coordinators to integrate and inform communications and information systems contingency planning and resilience efforts. (See AR 500–3 for additional information on COOP planning.)

*g. Contingency response team.* In general, a contingency response team is comprised of personnel who have been trained and are proficient at the assigned task or are subject matter experts for specific plan operations within the organization. The response team can evaluate effects of changes to ISCPs and should always be prepared to perform contingency measures to restore system functions.

*h. Risk management team.* The risk management team includes representatives of management, users, and cybersecurity. They carry out the tenets of the risk management program as prescribed in ATP 5–19 and DA Pam 385–30.

*i. Other possible information system contingency plan teams.* Other possible teams that could assist the ISCP coordinator to successfully plan and activate an ISCP are listed below. The types of teams required are based on the information system affected and could be tailored according to the assigned impact levels to reflect specific differences in requirements and backup procedures. The results of the BIA described in paragraph 3–3 should be incorporated into the analysis and strategy development efforts, and will help identify which ISCP teams are needed. The size of each team, team titles, and hierarchy designs depend on the organization. Furthermore, this list is not meant to be comprehensive. If the ISCP coordinator needs other teams, he or she should create them, as they are needed.

(1) Management team.

(2) Outage assessment team.

(3) Operating system administration team.

(4) Systems software team.

(5) Server recovery team (for example, client server, web server).

(6) Local area network/wide area network recovery team.

(7) Database recovery team.

(8) Network operations recovery team.

(9) Application recovery team(s).

(10) Telecommunications team.

(11) Hardware salvage team.

(12) Alternate site recovery coordination team.

- (13) Original site restoration/salvage coordination team.
- (14) Test team.
- (15) Administrative support team.
- (16) Transportation and relocation team.
- (17) Media relations team.
- (18) Legal affairs team.
- (19) Physical or personnel security team.
- (20) Procurement team.
- (21) External vendors for managed services.
- (22) Cloud service providers for commercial/government cloud services.

## **Chapter 3**

### **Information Technology Contingency Planning Process**

#### **3–1. Overview**

- a.* NIST SP 800–34 outlines a seven step process for contingency planning. The seven steps in the process are:
  - (1) Develop the contingency planning policy.
  - (2) Conduct the BIA.
  - (3) Identify preventive controls.
  - (4) Create contingency strategies.
  - (5) Develop an ISCP.
  - (6) Ensure plan testing, training, and exercises (TT&Es).
  - (7) Ensure plan maintenance.
- b.* The seven steps should be integrated into the SDLC to ensure ISCP requirements are properly identified and addressed throughout system development (see para 2–3).

#### **3–2. Develop the contingency planning policy**

- a.* To be effective and to ensure that personnel fully understand the organization’s contingency planning requirements, the contingency plan must be based on a clearly defined policy. AR 25–2 outlines the high-level policy requirements for contingency planning and continuity. The organization-level contingency planning policy statement should define the organization’s overall contingency objectives and establish the organizational framework and responsibilities for system contingency planning. The policy can be included as part of a general information security policy for the organization. Ensure the policy addresses IT and information protection requirements as outlined in AR 25–2.
- b.* The policy is developed and signed by the commander. This will ensure the program is supported by senior management. These officials can be included in the process to develop the program policy, structure, objectives, and roles and responsibilities.
- c.* At a minimum, the policy should comply with AR 25–2, the Federal Information Security Modernization Act of 2014 as outlined in NIST SP 800–53 and AR 500–3. These COOP requirements provide a good guide for ISCP requirements, as an ISCP often supports the timely performance of MEFs within the MTD of an organization’s COOP plan.
- d.* Organizations should evaluate their IT systems, operations, and requirements to determine if additional contingency planning requirements are necessary. Key policy elements for consideration include:
  - (1) Scope, as it applies to the type(s) of platform(s) and organization functions subject to contingency planning.
  - (2) Responsibilities.
  - (3) Resource requirements.
  - (4) Plan maintenance schedule.
  - (5) Frequency of backups and storage of backup media.
  - (6) Training requirements.
  - (7) Exercise and testing schedules.
- e.* As the policy and plan are developed, they should be coordinated with related and relevant organization activities, including:
  - (1) IT and physical security.
  - (2) Human resources.
  - (3) IT operations.

(4) Emergency preparedness functions. ISCP activities should be compatible with program requirements for these areas and contingency personnel should coordinate with representatives from each area to remain aware of new or evolving policies, programs, or capabilities.

### **3–3. Conduct a business impact analysis**

a. The BIA is a key step in implementing the contingency planning controls in NIST SP 800–53 and in the contingency planning process overall. The BIA enables the ISCP coordinator to characterize the system components, supported mission/business processes, and interdependencies. The BIA purpose is to correlate the system with the critical mission/business processes and services provided, and based on that information, characterize the consequences of a disruption. The ISCP coordinator can use the BIA results to determine contingency planning requirements and priorities. (See NIST SP 800–34 for more guidance on conducting and documenting a BIA.) The following steps are typically involved in accomplishing the BIA:

(1) *Determine mission/business processes and recovery criticality.* MEFs and business processes supported by the system are identified and the impact of a system disruption to those functions and processes is determined along with outage impacts and estimated downtime. The downtime should reflect the maximum time that an organization could tolerate while still maintaining the mission. Downtime can be identified in several ways:

(a) *Maximum tolerable downtime.* The MTD represents the total amount of time the system owner/authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave contingency planners with imprecise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail, which will be required when developing recovery procedures, including their scope and content.

(b) *Recovery time objective.* RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD. Because the RTO must ensure that the MTD is not exceeded, the RTO must normally be shorter than the MTD. For example, a system outage may prevent a particular process from being completed, and because it takes time to reprocess the data, that additional processing time must be added to the RTO to stay within the time limit established by the MTD. When it is not feasible to immediately meet the RTO and the MTD is inflexible, a plan of action and milestone should be initiated to document the situation and plan for its mitigation. The longer a disruption is allowed to continue, the more costly it can become to the organization and its operations. Conversely, the shorter the RTO, the more expensive the recovery solutions cost to implement. For example, if the system must be recovered immediately, zero downtime solutions and alternate processing site costs will be much higher, whereas a low-impact system with a longer RTO would require a less costly backup architecture.

(c) *Recovery point objective.* The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage. Unlike RTO, RPO is not considered as part of MTD. Rather, it is a factor of how much data loss the mission/business process can tolerate during the recovery process.

(2) *Identify resource requirements.* Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.

(3) *Identify recovery priorities for system resources.* Based upon the results from the previous activities, system resources can be linked more clearly to critical mission/business processes and functions. Priority levels can be established for sequencing recovery activities and resources.

(4) *Conduct a risk assessment.* After identifying system recovery priorities, the next step in the BIA is to perform an assessment to identify potential risks that could impact system availability, determine the likelihood of risks happening, assess the impact, and identify cost-effective mitigations. (See DA Pam 385–30, ATP 5–19, and NIST SP 800–30 for guidance on conducting a risk assessment.) The major outcomes from the risk assessment include:

(a) Understanding and estimation of the impact of downtime, which serves as justification for system recovery objectives.

(b) Identification of recovery objectives and a prioritized order for system components.

(c) Collection of information that may help identify appropriate current and future recovery strategies.

(d) Understanding of potential risks, including their likelihood and impact.

(e) Identification of existing controls, and potential control enhancements or new strategies to mitigate risk by protecting resources (as to decrease the likelihood or severity associated with a disruptive incident).

(f) Information on the effectiveness of proposed or existing controls, as well as any additional controls or actions to decrease the likelihood or severity of a system disruption.

(g) A risk management strategy or validation of an existing one with the goal to ensure alternate methods are identified to mitigate potential risks and threats that would cause a system disruption.

(h) Information for leadership to make informed decisions about acceptable and unacceptable risk that drives the expenditure of resources to mitigate these risks.

b. The ISCP coordinator, working with management, should determine the optimum point to recover the information system while balancing the cost of system inoperability against the cost of resources required for restoring the system and its overall support for critical mission/business processes. The ISCP coordinator should also consult with organization COOP points of contact to ensure that MEF prioritization and continuity planning requirements are integrated with this process. (See AR 500–3 for additional information on ISCP and COOP planning integration.)

### 3–4. Identify preventive controls

In some cases, the outage impacts identified in the BIA may be mitigated or eliminated through preventive measures that deter, detect, and/or reduce impacts to the system. Where feasible and cost-effective, preventive methods are preferable to actions that may be necessary to recover the system after a disruption. Step 2 of the RMF (select security controls) includes the identification of effective contingency planning preventive controls and maintaining these controls on an ongoing basis. A variety of preventive controls is identified in NIST SP 800–53, depending on system type and configuration. Preventive controls include, but are not limited to:

a. Appropriately, sized uninterruptible power supplies (UPSs) to provide short-term backup power to all system components (including environmental and safety controls).

b. IT design changes or technical controls useful in precluding or reducing continuity issues.

c. Gasoline-powered, diesel-powered, or natural gas generators to provide long-term backup power.

d. Air-conditioning systems with adequate excess capacity to accommodate failure of certain components, such as a compressor.

e. Fire detection and suppression systems.

f. Water sensors in the computer room ceiling and floor.

g. Plastic tarps that may protect IT equipment from water damage.

h. Heat-resistant and waterproof containers for backup media and vital nonelectronic records.

i. Emergency master system shutdown switch.

j. Offsite storage of backup media, nonelectronic records, and system documentation.

k. Technical security controls, such as cryptographic key management and least-privilege access controls.

l. Frequent, scheduled backups.

m. Environmental control monitoring systems.

### 3–5. Create contingency strategies

a. *Mitigating risks.* Organizations are required to adequately mitigate the risk arising from use of information and information systems in the execution of mission/business processes. The challenge for organizations is in implementing the right set of security controls. Guided by the RMF and in accordance with CNSSI 1253 and NIST SP 800–53, security controls are selected and implemented. Contingency strategies are created to mitigate the risks for the contingency planning family of controls and cover the full range of backup, recovery, contingency planning, testing, and ongoing maintenance.

b. *Backup and recovery strategies.* Backup and recovery strategies provide a way to restore IT operations quickly and effectively following a service disruption. The strategies should address disruption impacts and allowable outage times identified in the BIA. Several alternatives should be considered when developing the recovery strategy including cost, allowable outage time, security, and integration with larger, organization-level ISCPs and the MTD of supported MEF requirements of COOP plans. Plans should consider in place and displaced responses. When disruption occurs, there should be immediate actions to take that anticipate recovery in place. Likewise, planning considerations for eventual displacement and include strategies for the secondary location; warm and hot sites. For example, various power remedies should be explored, developed, and planned for in place resolution. Considerations should also include the approaches below.

(1) A wide variety of approaches may be considered; the appropriate choice depends on the incident, type of system, and its operational requirements. It is important to balance the costs of the recovery with the length of time planned for recovery. To do this, a recovery strategy budget-planning guide is provided in table 3–2. A good general recovery strategy:

(a) Addresses potential impacts identified in the BIA.

- (b) Integrates the system architecture during the design and implementation phases of the system lifecycle.
- (c) Includes a combination of methods to provide recovery capability over the full spectrum of incidents.
- (d) Uses established backup methods and alternate sites to connect to the backup, if the backup does not have a front-end physical connection site for employees.

(2) Developing the data backup strategy.

(a) *Requirements.* Backup is required by both DoD and Federal statute. To what extent and how often depends on the category of the system. Utilize the system's CNSSI 1253 security categorization and assigned controls as the baseline for backup strategies.

(b) *Backup policy.* The most effective data backup policy designates the location of stored data, file-naming conventions, frequency of backups (for example, daily or weekly, incremental or full), and methods for transporting data offsite. The protection and ready availability of electronic and hardcopy emergency operating records, documents, references, records, and information systems needed to support MEFs at an alternate site under the full spectrum of emergencies is a critical element of a successful ISCP. Personnel should have access to and be able to use these records and systems in conducting their essential functions. Refer to DA Pam 25-403 for more information.

(c) *Data storage media.* Data may be backed up on magnetic disk, tape, or optical discs (such as compact discs (CDs)). The specific method chosen for conducting backups should be based on system and data availability and integrity requirements refer to AR 380-5 for specific guidelines on security of this material.

(d) *Off-site storage.* It is a good business practice to store backed up data offsite. If your system is supported in everyday operations in an area-processing center (APC), there is an option to have your system backup to alternate APCs. This would be part of the service level agreement (SLA) as described in paragraph 3-5b(2).

(e) *Equipment replacement.* If the IT system is damaged or destroyed, or the primary site is unavailable, necessary hardware and software will need to be activated or procured quickly and delivered to the alternate location. When selecting the most appropriate strategy, note that the availability of transportation may be limited or temporarily halted in the event of a catastrophic disaster.

(f) *Vendor agreements.* Agreements with hardware, software, and support vendors may be made for emergency maintenance service. The agreements should specify the requirements in paragraph 3-5b(2).

(g) *Equipment inventory.* Required equipment may be purchased in advance and stored at a secure off-site location, such as an alternate site where recovery operations will take place (warm or mobile site) or at another location where they will be stored and then shipped to the alternate site. This solution has certain drawbacks, however. An organization must commit financial resources to purchase this equipment in advance and the equipment could become obsolete or unsuitable for use over time because system technologies and requirements change.

(h) *Existing compatible equipment.* Equipment currently housed and used by the contracted hot site or by another organization within the agency may be used by the organization. Agreements made with hot sites and reciprocal internal sites stipulate that similar and compatible equipment will be available for contingency use by the organization.

(i) *Procedures.* Most importantly, backup procedures should be implemented into the daily routine of an office. This will ensure all parties involved know where the information is going and ensure their information has a backup.

(j) *Access.* Having a backup policy for the system does not alone ensure COOP. Access to the information is also needed. For more information, refer to paragraphs 3-5b and 3-5c, of this pamphlet.

c. *Establish alternate sites.* As stated in the CNSSI 1253 security categorization for the availability security objective determines which alternate site contingency planning controls apply to a particular system. Although major disruptions with long-term effects may be rare, they should be accounted for in the ISCP. Thus, for all moderate or high-impact systems, the plan should include a strategy to recover and perform system operations at an alternate facility for an extended period. Organizations may consider low-impact systems for alternate site processing, but that is an organizational decision and not required. The selection of the type of site should be based on the organizations BIA, cost, and requirements of the system. Table 3-1 summarizes the criteria which can be employed to determine which type of alternate site meets the organization's requirements. Table 3-2 gives a basic outline of costs associated with contingency planning.

(1) Alternate sites can contain the system backup hardware or could be a remote site that is, in essence, teleworking from an off-site location, also known as a teleworking site. In general, three types of alternate sites are available:

- (a) Dedicated site-owned or site-operated by the organization.
- (b) Reciprocal agreement or memorandum of agreement with an internal or external entity.
- (c) Commercially leased facility.

(2) Once selected, the above three site types can be further categorized into one of the five below categories in accordance with their operational readiness progressing from basic to advanced.

(a) *Cold site.* Typically consists of a facility with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support the IT system.



(b) *Warm site.* Partially equipped spaces that contain some or all of the system hardware, software, telecommunications, and power sources. The warm site is maintained in an operational status, ready to receive the relocated system. In many cases, a warm site may serve as a normal operational facility for another system or function, and in the event of ISCP activation, the normal activities are displaced temporarily to accommodate the disrupted system.

(c) *Hot site.* Spaces appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel. Hot sites are typically staffed 24 hours a day, 7 days a week.

(d) *Mobile site.* Self-contained, transportable shells custom-fitted with specific telecommunications and IT equipment necessary to meet system requirements.

(e) *Mirrored site.* Fully redundant facilities with full, real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects.

**Table 3–1**  
**NIST SP 800–34 sample alternate site criteria**

Site	Cost	Hardware Equipment	Telecommunications	Setup Time	Location
Cold Site	Low	None	None	Long	Fixed
Warm Site	Medium	Partial	Partial/Full	Medium	Fixed
Hot Site	Medium/High	Full	Full	Short	Fixed

(3) *Service level agreements.* A memorandum of understanding, memorandum of agreement, operational level agreement, or an SLA for an alternate site or backup processing should be developed specific to the organization's needs and the partner organization's capabilities. It is up to the ISCP coordinator to decide which agreement is most relevant. The legal department of each party must review and approve the agreement. (See NIST SP 800–34 for the elements that need to be addressed in the SLA.)

(a) Be aware that multiple organizations may contract with a vendor for the same alternate site; as a result, the site may be unable to accommodate all of the customers if a disaster affects enough of those customers simultaneously. The vendor's policy on how this situation should be addressed and how priority status is determined should be negotiated.

(b) Two or more organizations with similar or identical IT configurations and backup technologies may enter a formal agreement to serve as alternate sites for each other or enter into a joint contract for an alternate site. This type of site is set up through a reciprocal agreement or memorandum of understanding. A reciprocal agreement should be entered into carefully because each site must be able to support the other in addition to its own workload in the event of a disaster. This type of agreement requires the recovery sequence for the applications from both organizations to be prioritized from a Joint perspective, favorable to both parties.

(c) Alternate site and emergency communications: the success of organizational operations at an alternate facility is dependent on the availability and redundancy of critical communications systems to support connectivity to internal organizations, other agencies, critical customers, and the public. When identifying communications requirements, agencies should take maximum advantage of the entire spectrum of communications media likely to be available in any emergency situation. These services may include, but are not limited to: secure and/or non-secure voice, fax, and data connectivity; internet access; and email. Interoperable communications should provide:

1. Capability commensurate with an organization's MEFs and activities.
2. Ability to communicate with the ISCP staff, management, and other organizational components.
3. Ability to communicate with other agencies and emergency personnel.
4. Access to other data and systems necessary to conduct essential activities and functions.

(d) It is essential that emergency communications planning prepare for the absence of email capability due to a loss of local area network or wide area network connectivity. Access to other communication methods such as cellular/wireless, including secure voice phones, Iridium, land mobile radios, and International Maritime Satellite/Enhanced Mobile Satellite services may be helpful for ISCP coordinators. It is recommended that at least some of the personnel responsible for carrying out the ISCP have access to cellular phones and wireless devices that have had wireless priority service added to them. Similarly, those personnel should have access to the government emergency telephone service. In previous contingency scenarios, landline service was non-existent and cellular and wireless networks soon became congested. Wireless priority service and government emergency telephone service both assist essential and first responder personnel in getting calls through.

*d. Leverage teleworking for displaced employees.* Teleworking policy and procedures should already be addressed in the COOP plan and should be factored into the ISCP. The ISCP should address alternate VPN connection sites if the primary VPN site is impacted by the outage. Telework provides flexibility in the locations where employees may perform their jobs. Telework lets employees work at home, at an alternate office closer to home, or at other defined telework locations as established during an alternate site designation. Telework may be performed on a fixed schedule or at random. For the Army, perhaps the most important aspect of telework is that it can greatly facilitate the ISCP in times of crises, to include times of a pandemic health crisis in which direct contact is discouraged. See AR 25–1 and DA Pam 25–1–1 for additional telework policy and procedures. Designated contingency facilities may not have all the staff needed to support MEFs and may not be able to accommodate enough key staff to facilitate maximum Government operations. Organizations should make sure that key members of the staff are designated to report to alternate sites, including their home, if they telework.

**Table 3–2**  
**Recovery strategy budget planning example (in dollars)**

		Vendor Costs	Hardware Costs	Software Costs	Travel/ Shipping Costs	Labor/ Contractor Costs	Testing Costs	Supply Costs	Totals
Alternate Site	Cold Site	25,000	30,000	3,000	15,000	20,000	2,000	10,000	105,000
	Warm Site	50,000	40,000	4,000	10,000	15,000	3,000	8,000	130,000
	Hot Site	75,000	45,000	4,500	5,000	10,000	4,000	5,000	148,500
	Mobile Site	75,000	45,000	4,500	8,000	15,000	4,000	5,000	156,500
	Mirrored Site	50,000	40,000	4,000	5,000	10,000	3,000	3,000	115,000
Offsite Storage	Commercial	100,000	0	0	5,000	10,000	4,000	3,000	122,000
	Internal	25,000	30,000	3,000	0	0	2,000	2,000	62,000
Equipment Replacement	SLAs	25,000	30,000	15,000	0	10,000	3,000	0	83,000
	Storage	20,000	20,000	5,000	0	0	0	0	45,000
	Existing Use	0	50,000	3,000	3,000	0	2,000	2,000	60,000

### 3–6. Develop the information system contingency plan

*a.* In general, each organization develops and implements a contingency plan that addresses contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Rapidly changing technologies and cyber threats make it important that ISCPs are kept accurate and organized so the most important content can be quickly accessed or updated. For example, numerous RMF items specify a personnel roster. Instead of having multiple rosters in different files, it can be more practical to maintain a centralized roster accessible to all users and additional/backup copies where needed.

*b.* NIST SP 800–34 identifies five main components of the contingency plan: supporting information, activation and notification phase, recovery phase, reconstitution phase, and appendixes. The supporting information and plan appendixes provide essential information to ensure a comprehensive plan. The activation and notification, recovery, and reconstitution phases address specific actions that the organization should take following a system disruption or emergency.

(1) *Supporting information.* The supporting information of the plan should include an introduction and concept of operations (CONOPS) section that provides essential background or contextual information that makes the contingency plan easier to understand, implement, and maintain. The introduction subsections generally address the ISCP background, scope, and assumptions. The plan CONOPS may include the system description, roles and responsibilities, and an overview of the three ISCP phases that will be outlined in more detail in the rest of the document.

(2) *Activation and notification phase.* This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to the system. Based on the assessment of the event, the plan may be activated by the designated authority. The ISCP elements that address this phase include:

- (a) Activation criteria.
- (b) Activation authority.

- (c) Notification procedures.
- (d) Outage assessment.
- (3) *Recovery phase*. This phase focuses on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or alternate site. The ISCP elements that address this phase include:
  - (a) Recovery strategy.
  - (b) Sequence of recovery activities.
  - (c) Recovery procedures.
  - (d) Recovery escalation.
- (4) *Reconstitution phase*. This phase defines the actions taken to test and validate system capability and functionality. During reconstitution, recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. This phase consists of two major activities: validating successful recovery and deactivation of the plan.
  - (a) *Validation of recovery*. Validation of recovery includes concurrent processing, validation data testing, and validation functionality testing.
  - (b) *Plan deactivation*. Deactivation procedures return the system to normal operations and finalize reconstitution activities to prepare the system against another outage or disruption. Deactivation activities include:
    1. Notifications of the return to normal operations.
    2. Cleanup.
    3. Offsite data storage.
    4. Data backup.
    5. Event documentation.
  - (5) *Plan appendixes*. The plan appendixes provide key details not contained in the main body of the plan. A list of recommended appendixes is provided in the ISCP templates referenced in paragraph 3–6c.
- c. Refer to NIST SP 800–34, the DoD RMF Knowledge Service (available at <https://rmfks.osd.mil>), and AR 500–3 for more detailed guidance on preparing the components and content of a contingency plan. Free sample ISCP templates are available at <https://csrc.nist.gov/publications/detail/sp/800–34/rev-1/final> and <http://www.ias-sure.com/products/rmf-templates/>. The information and templates provided are guides and may be modified, customized, and/or adapted as necessary to best meet the specific system, operational, and organizational requirements for contingency planning.

### 3–7. Plan testing, training, and exercises

- a. TT&E help to determine the plan’s effectiveness and the organization’s readiness to execute the plan. This includes having personnel trained to fulfill their roles and responsibilities within the plan, having plans exercised to validate their content, and having systems and system components tested to ensure their operability in the environment specified in the ISCP. Appropriate officials review the contingency plan test results and initiate corrective actions. Additionally, the organization can coordinate contingency plan testing with organizational elements responsible for related plans (for example, business continuity plan, disaster recovery plan, COOP plan, business recovery plan, and incident response plan). Army COOP programs are also required to develop TT&E plans. Aligning ISCP TT&E events with COOP TT&E events identifies opportunities to test ISCPs when personnel are at continuity facilities. Another good business practice, if applicable, is testing the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site’s capabilities to support contingency operations.
- b. Planned testing is a critical element of a viable ISCP and will be conducted at least annually. Testing enables plan deficiencies to be identified and addressed. ISCP testing should occur prior to funding cycles to ensure proper funding is identified to address deficiencies. Testing also helps evaluate the ability of the recovery staff to implement the plan quickly and effectively. Each ISCP element should be tested to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan. This will be confirmed or denied by an after action review and report.
- c. The most effective ISCP test will include, at a minimum:
  - (1) Notification procedures.
  - (2) Coordination among recovery teams.
  - (3) Systems recovery on an alternate platform from backup media.
  - (4) Internal and external connectivity.
  - (5) Systems performance using alternate equipment.

(6) Restoration of normal operations.

(7) After action review and report.

d. The following list contains the types of acceptable exercises used in ISCP testing:

(1) *Tabletop*. Contingency response team members are alerted or assembled to a location and allowed a certain quantity of time to work through a contingency scenario. This type of training is the easiest and least expensive method in which to test emergency preparedness. Tabletop exercises are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants of roles, responsibilities, coordination, and decision-making. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources. Tabletop exercises are NOT acceptable evidence of successful IT system failover/failback certification for moderate or high impact systems.

(2) *Functional testing and system testing*. System testing entails utilizing only a portion of the contingency response team and is limited to a specific system or process. This type of testing is excellent for instituting new systems, or new procedures for old systems, into the continuity plan. System testing can also be used to test and train on failover hardware and procedures. For example, a failover test can be conducted on redundant firewall modules in a router. Functional exercises allow personnel to validate their operational readiness for emergencies by performing their duties in a simulated operational environment. Functional exercises are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (for example, communications, emergency notifications, system equipment setup). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements. Functional exercises allow staff to execute their roles and responsibilities as they would in an actual emergency situation, but in a simulated manner.

e. A thorough after action review should be conducted with all individuals involved in the testing and training event.

(1) ISCP documentation should be updated and a full report filed, to include lessons learned.

(2) Action items should be assigned to team members and all deliverables tracked.

(3) Procedures found to be inadequate should be documented, changed, and retested as soon as feasible.

(4) Information collected during the test and post-test reviews that improve plan effectiveness should be incorporated into the ISCP.

(5) The ISCP coordinator should record plan modifications using a record of changes, which lists the page number, change comment, and date of change.

f. Announcing the test in advance is a benefit to team members so they can prepare for it mentally and have time to prioritize their workload. It is likely that some team members will not be available because of absence or because the test may be disruptive to their workload. Documenting personnel availability issues will benefit the plan by capturing how a real response may play out, thus providing critical input to plan modifications. Exercising the ISCP should not disrupt normal operations. If testing at the alternate facility, the ISCP coordinator should coordinate test dates and operations with the facility.

g. Training for personnel with ISCP responsibilities should complement testing. The DoD RMF implementation guidelines for contingency planning training are to provide initial training within 10 working days for personnel with newly assigned ISCP duties and refresher training at least annually.. Ultimately, ISCP personnel should be trained to the extent that they are able to execute their respective recovery procedures without aid of the actual document. This is an important goal in the event that paper or electronic versions of the plan are unavailable for the first few hours resulting from the extent of the disaster. Recovery personnel should be trained on the following plan elements:

(1) Purpose of the plan.

(2) Cross-team coordination and communication.

(3) Reporting procedures.

(4) Security requirements.

(5) Team-specific processes (notification/activation, recovery, and reconstitution phases).

(6) Individual responsibilities (notification/activation, recovery, and reconstitution phases).

(7) Archival procedures.

h. The depth and rigor of ISCP TT&E activities increases with the system availability security objective. All tests and exercises should include some kind of determination of the effects on the organization's operations and provide for a mechanism to update and improve the plan as a result.

(1) For low-impact systems, a tabletop exercise at an organization-defined frequency is sufficient. The tabletop should simulate a disruption, include all main ISCP points of contact, and be conducted by the system owner or responsible authority.

(2) For moderate-impact systems, a functional exercise at an organization-defined frequency should be conducted. The functional exercise should include all ISCP points of contact and be facilitated by the system owner or responsible authority. Exercise procedures should be developed to include an element of system recovery from backup media.

(3) For high-impact systems, a full-scale functional exercise at an organization-defined frequency should be conducted. (See AR 500–3 for systems essential for COOP.) The full-scale functional exercise should include a system failover to the alternate location. This could include additional activities such as full notification and response of key personnel to the recovery location, recovery of a server or database from backup media or setup, and processing from a server at an alternate location. The test should also include a full recovery and reconstitution of the information system to a known state.

### **3–8. Information system contingency plan maintenance**

a. Because the ISCP contains potentially sensitive operational and personnel information, its distribution should be marked accordingly and controlled according to AR 380–5. COOP plans are frequently classified and ISCPs that support a classified COOP plan may contain classified information. Check with the respective organizational COOP planner. Classified ISCPs must be stored and protected per their classification.

b. Typically, copies of the plan are provided to recovery personnel. A copy should also be stored at the alternate site and with the backup media. Storing a copy of the plan at the alternate site ensures its availability and good condition in the event local plan copies cannot be accessed because of the disruption. The ISCP coordinator should ensure that any revisions to the ISCP are reflected in the document provided to recovery personnel and stored at the alternate site. The ISCP coordinator should maintain a record of copies of the plan and to whom the plan was distributed.

c. To be effective, the plan must be maintained in a state of readiness that accurately reflects system requirements, procedures, organizational structure, and policies. IT systems undergo frequent changes because of shifting business needs, technology upgrades, or new internal or external policies. As a general rule, the plan should be reviewed for accuracy and completeness at least annually prior to testing or whenever significant changes occur to any element of the system, capability or plan. Certain elements will require more frequent reviews, such as contact lists and hardware. Evaluate supporting information to ensure the information is current and continues to meet system requirements adequately. This information includes the following:

- (1) Names and contact information of team members.
- (2) Alternate site contract, including testing times.
- (3) Off-site storage contract.
- (4) Software licenses.
- (5) Memorandums of understandings or vendor SLAs and POC information related to them.
- (6) Hardware and software requirements.
- (7) System interface agreements.
- (8) Security requirements.
- (9) Recovery strategy.
- (10) Based on the system type, criticality, and changes to hardware, firmware, software, or network configurations, ISCP content and procedures must be evaluated/tested more frequently than annually. At a minimum, plan reviews should focus on the following elements:
  - (11) Operational requirements.
  - (12) Security requirements.
  - (13) Technical procedures.
  - (14) Vital records (electronic and hardcopy).
  - (15) Alternate and offsite facility requirements.

d. The ISCP coordinator should record plan modifications using a record of changes, which lists the page number, change comment, and date of change. Changes to the ISCP should be communicated to representatives of associated plans or programs, as necessary.

e. Although some changes may be quite visible, others will require additional analysis. The BIA should be reviewed periodically and updated with new information to identify new contingency requirements or priorities. As new technologies become available, preventive controls may be enhanced and recovery strategies may be modified.

f. The ISCP coordinator should coordinate frequently with associated internal and external organizations and system POCs to ensure that impacts caused by changes within either organization will be reflected in the contingency plan. COOP plans are required to be updated whenever there is a mission change or every 2 years. Strict version

control should be maintained by requesting old plans or plan pages to be returned to the ISCP coordinator in exchange for the new plan or plan pages.

g. The ISCP coordinator should refer to AR 380–5 for information pertaining to the protection of information stored at the site of a contingency situation. More specifically, plans should be in place to monitor emergency personnel so classified material is accounted for as part of the damage assessment phase.

## **Appendix A**

### **References**

#### **Section I**

##### **Required Publications**

###### **AR 25–1**

Army Information Technology (Cited in para 1–1.)

###### **AR 25–2**

Army Cybersecurity (Cited in para 1–1.)

###### **AR 70–1**

Army Acquisition Policy (Cited in para 1–1.)

###### **AR 70–75**

Survivability of Army Personnel and Materiel (Cited in para 2–1*c*.)

###### **AR 190–13**

The Army Physical Security Program (Cited in para 1–1.)

###### **AR 190–51**

Security of Unclassified Army Property (Sensitive and Nonsensitive) (Cited in para 1–1.)

###### **AR 380–5**

Army Information Security Program (Cited in para 2–4*d*(10).)

###### **AR 500–3**

U.S. Army Continuity of Operations Program Policy and Planning (Cited in para 1–1.)

###### **ATP 5–19**

Risk Management (Cited in para 2–4*h*.)

###### **CNSSI 1253**

Security Categorization and Control Selection for National Security Systems (Cited in para 1–1.) (Available at <https://www.cnss.gov/cnss/issuances/instructions.cfm>.)

###### **DA Pam 25–1–1**

Army Information Technology Implementation Instructions (Cited in para 2–1*d*.)

###### **DA Pam 25–2–14**

Risk Management Framework for Army Information Technology (Cited in para 2–2*b*.)

###### **DA Pam 25–403**

Guide to Recordkeeping in the Army (Cited in para 3–5*b*(2)(*b*).)

###### **DA Pam 190–51**

Risk Analysis for Army Property (Cited in para 1–1.)

###### **DA Pam 385–30**

Risk Management (Cited in para 2–4*h*.)

###### **DoD Senior Information Security Officer memorandum**

Contingency Planning for DOD Information Systems (Cited in para 1–1.) (Available at [https://army.deps.mil/army/cmds/hqda\\_ciog6/memos/contingency%20planning%20for%20dod%20info%20sys-tems%2020june2019.pdf](https://army.deps.mil/army/cmds/hqda_ciog6/memos/contingency%20planning%20for%20dod%20info%20sys-tems%2020june2019.pdf).)

###### **DoDI 8500.01**

Cybersecurity (Cited in para 1–1.) (Available at <http://www.esd.whs.mil/dd/dod-issuances/>.)

###### **NIST SP 800–30**

Guide for Conducting Risk Assessments (Cited in para 3–3*a*(4).) (Available at <https://csrc.nist.gov/publications/sp>.)

###### **NIST SP 800–34**

Contingency Planning Guide for Federal Information Systems, Revision 1 (Cited in para 2–3*g*.) (Available at <https://csrc.nist.gov/publications/sp>.)

**NIST SP 800–53**

Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4 (Cited in para 1–1.)  
(Available at <https://csrc.nist.gov/publications/sp>.)

**Section II****Related Publications**

A related publication is a source of additional information. The user does not have to read it to understand this publication.

**AR 525–26**

Infrastructure Risk Management (Army)

**DoDD 3020.26**

DoD Continuity Policy (Available at <https://www.esd.whs.mil/dd/dod-issuances/>.)

**DoDI 3020.42**

Defense Continuity Plan Development (Available at <https://www.esd.whs.mil/dd/dod-issuances/>.)

**Federal Continuity Directive 1**

Federal Executive Branch National Continuity Program and Requirements (Available at <https://www.fema.gov/media-library/assets/documents/86284>.)

**Federal Information Security Modernization Act (FISMA) of 2014**

(Available at <https://www.congress.gov/bill/113th-congress/senate-bill/2521/text>.)

**OMB Circular A–130**

Managing Federal Information as a Strategic Resource (Available at <https://www.whitehouse.gov/omb/circulars/>.)

**Section III****Prescribed Forms**

This section contains no entries.

**Section IV****Referenced Forms**

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate (APD) website (<https://armypubs.army.mil>).

**DA Form 2028**

Recommended Changes to Publications and Blank Forms



## **Glossary**

### **Section I**

#### **Abbreviations**

**APC**

area-processing center

**APMS**

Army Portfolio Management Solution

**AR**

Army regulation

**ATP**

Army Techniques Publication

**BIA**

business impact analysis

**CONOPS**

concept of operations

**COOP**

continuity of operations

**DA Pam**

Department of the Army pamphlet

**DoD**

Department of Defense

**DoDD**

Department of Defense directive

**DoDI**

Department of Defense instruction

**IA**

information assurance

**IS**

Information System

**ISCP**

Information System Contingency Plan

**ISO**

information system owner

**IT**

information technology

**MC**

mission critical

**ME**

mission essential

**MEF**

mission essential function

**MTD**

maximum tolerable downtime

**NIST**

National Institute of Standards and Technology

**PEO**

program executive officer

**PIT**

platform information technology

**PM**

program manager

**POC**

point of contact

**RMF**

risk management framework

**RPO**

recovery point objective

**RTO**

recovery time objective

**SDLC**

system development life cycle

**SLA**

service level agreement

**SP**

Special Publication

**TT&E**

testing, training, and exercise

**Section II****Terms****Alternate site**

A location to recover and perform system operations for an extended period in the event of an ISCP implementation. In general, three types of alternate sites are available: (1) A dedicated site owned or operated by the organization; (2) A site reserved through reciprocal agreement or memorandum of agreement with an internal or external entity; (3) A commercially leased facility.

**Business continuity plan**

The business continuity plan focuses on sustaining an organization's business functions during and after a disruption. IT systems are considered in the business continuity plan in terms of their support to the business processes. The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.

**Business impact analysis**

An analysis of IT system's requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

**Cold site**

These sites typically consist of a facility with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support the IT system. The space may have raised floors and other attributes suited for IT operations. The site does not contain IT equipment and usually does not contain office automation equipment, such as telephones, facsimile machines, or copiers. The organization using the cold site is responsible for providing and installing necessary equipment and telecommunications capabilities. A backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternate site.

**Concept of operations**

A verbal or graphic statement, in broad outline, of a commander's assumptions or intent in regard to an operation or series of operations. The CONOPS frequently is embodied in campaign plans and operation plans; in the latter case, particularly when the plans cover a series of connected operations to be carried out simultaneously or in succession. The concept is designed to give an overall picture of the operation. It is included primarily for additional clarity of purpose. Also called commander's concept or CONOPS. A verbal or graphic statement that clearly and concisely expresses what the commander intends to accomplish and how it will be done using available resources.

**Continuity of operation**

An internal effort within individual organizations to ensure uninterrupted, missions essential functions across a wide range of potential emergencies, including localized acts of nature, accidents, and technological and/or attack-related emergencies. The level in which there is a continuous commitment in the conduct of functions, tasks, or duties necessary to accomplish a military action or mission in carrying out national military strategy. It includes the functions and duties performed by the commander, his or her staff, and others acting under the authority and direction of the commander. The degree or state of being continuous in the conduct of functions, tasks, or duties necessary to accomplish a military action or mission in carrying out the national military strategy.

**Continuity of operation plan**

A plan focused on executing an organization's MEFs at an alternate site(s) within 12 hours and performing those MEF for up to 30 days after a disaster event before returning to normal operations.

**Continuity of support/information technology contingency plan**

Plans for general support systems and contingency plans for major applications. Because an IT contingency plan should be developed for each major application and general support system, multiple contingency plans may be maintained within the organization's business continuity plan.

**Differential backup**

A differential backup stores files that were created or modified since the last full backup.

**Disaster recovery planning**

A disaster recovery plan applies to major, usually catastrophic, events that deny access to the normal facility for an extended period. Frequently, disaster recovery planning refers to an IT-focused plan designed to restore operability of the target systems, applications, and an IT contingency plan; however, the disaster recovery planning is narrower in scope and does not address minor disruptions that do not require relocation.

**Full backup**

A full backup captures all files on the disk or within the folder selected for backup. Because all backed-up files were recorded to a single media or media set, locating a particular file or group of files is simple. However, the time required to perform a full backup can be lengthy. In addition, full backups of files that do not change frequently (such as system files) could lead to excessive, unnecessary media storage requirements.

**Hot site**

Hot sites are office spaces appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel. Hot sites are typically staffed 24 hours a day, 7 days a week. Hot site personnel begin to prepare for the system arrival as soon as they are notified that the contingency plan has been activated. A fully operational offsite data processing facility equipped with hardware and software, to be used in the event of an information system disruption.

**Incremental backup**

An incremental backup captures files that were created or changed since the last backup, regardless of backup type. Incremental backups afford more efficient use of storage media, and backup times are reduced. However, to recover a system from an incremental backup, media from different backup operations may be required. For example, consider a case in which a directory needed to be recovered. If the last full backup was performed three days prior and one file had changed each day, then the media for the full backup and for each day's incremental backups would be needed to restore the entire directory.

**Information system**

The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. For the purposes of APMS-AITR, the terms "application" and "information system" are used synonymously—a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information. The application of IT to solve a business or

operational (tactical) problem creates an information system. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

**Information system owner**

Person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system.

**Information technology contingency planning policy statement**

A formal organization policy that provides the authority and guidance necessary to develop an effective contingency plan.

**Internet backup/online backup**

Internet backup, or online backup, is a strategy that allows PC users to back up data to a remote location over the Internet. A utility is installed onto the PC that allows the user to schedule backups, select files and folders to be backed up, and establish an “archiving” scheme to prevent files from being overwritten. Data can be encrypted for transmission; however, this will impede the data transfer speed over a modem connection. The advantage of Internet Backup is that the user is not required to purchase data backup hardware or media.

**Maximum tolerable downtime**

The total amount of time the mission owner is willing to accept for a mission/business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave contingency planners with imprecise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail which will be required when developing recovery procedures, including their scope and content.

**Mirrored site**

Mirrored sites are fully redundant facilities with full, real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects. These sites provide the highest degree of availability because the data is processed and stored at the primary and alternate site simultaneously. These sites typically are designed, built, operated, and maintained by the organization.

**Mission essential functions**

A function that is vital to the continuation of operations of the organization. These functions include those required by statute or Executive Order, and other functions deemed essential by the head of each organization. MEFs are those continuing activities that must be performed without interruption to execute critical missions. MEFs are prioritized, which allows for a graduated response and relocation to the alternate continuity facilities with minimum interruptions to operations during a national/local emergency or during normal operations.

**Mobile site**

Mobile sites are self-contained, transportable shells custom-fitted with specific telecommunications and IT equipment necessary to meet system requirements. These are available for lease through commercial vendors. The facility often is contained in a tractor-trailer and may be driven to and setup at the desired alternate location. In most cases, to be a viable recovery solution, mobile sites should be designed in advance with the vendor, and an SLA should be signed between the two parties. This is necessary because the time required to configure the mobile site can be extensive, and without prior coordination, the time to deliver the mobile site may exceed the system’s allowable outage time.

**Notification/activation phase**

This phase defines the initial actions taken once a system disruption or emergency has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, assess system damage, and implement the plan.

**Platform information technology**

IT, both hardware and software, that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems. PIT has a single purpose, that is, to support the operations of the platform on which it resides. If removed from the platform, it has no function or purpose. Examples of platforms that may include PIT are weapons systems, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical devices and health ITs, vehicles and alternative fueled vehicles (for example, electric, bio-fuel, liquid natural gas) that contain car computers, buildings and their associated control systems (building automation systems or building management systems, energy management system, fire and life safety, physical security, elevators, and so forth), utility distribution systems (such as electric, water, waste water, natural gas and steam), telecommunications systems designed specifically for control systems including supervisory control and data acquisition, direct digital control, programmable logic controllers, other control

devices, and advanced metering or sub-metering and their associated data transport mechanisms (for example, data links and dedicated networks).

#### **Platform information technology system**

A collection of PIT within an identified boundary under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location. Owners of PIT, in consultation with an AO, may determine that a collection of PITs rise to the level of a PIT system. PIT systems are analogous to enclaves but are dedicated only to the platforms they support. PIT systems must be designated as such by the responsible agency heads or their delegates and authorized by an AO specifically appointed to authorize PIT systems.

#### **Potential impact category**

Security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.

#### **Recovery phase**

The recovery phase is the segment of the IT contingency plan in which activities focus on contingency measures to execute temporary IT processing capabilities, repair damage to the original system, and restore operational capabilities at the original or new facility.

#### **Recovery point objective**

The RPO is the point in time in which data must be restored in order to resume processing.

#### **Recovery time objective**

The RTO is the maximum acceptable length of time that elapses before the unavailability of the system severely affects the organization.

#### **Risk assessment**

A risk assessment identifies an organization's information assets and the threats to each asset. The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

#### **Risk management**

Risk management is not an event, it is a process. An ongoing commitment is essential to effective risk management. Risk management includes an array of activities used to identify, control, and mitigate risks to IT systems and the ability to provide IT services. The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (1) establishing the context for risk-related activities; (2) assessing risk; (3) responding to risk once determined; and (4) monitoring risk over time.

#### **Service level agreement**

A formal agreement between the customer(s) and the service provider specifying service levels and the terms under which a service or a package of services is provided to the customer.

#### **Vital records**

The records, databases, documents, references, records, and information systems needed to support MEFs during a continuity event that includes those records and information systems necessary for reconstitution to normal operations after the event.

#### **Warm site**

Warm sites are partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources. The warm site is maintained in an operational status ready to receive the relocated system. The site may need to be prepared before receiving the system and recovery personnel. In many cases, a warm site may serve as an operational facility for another system or function, and in the event of contingency plan activation, the standard activities are displaced temporarily to accommodate the disrupted system. An environmentally conditioned work space that is partially equipped with information systems and telecommunications equipment to support relocated operations in the event of a significant disruptions.

**UNCLASSIFIED**

**PIN 083586-000**