



Standard Operating Procedure

Contingency Planning Guidance

ITS-SOP-0040 Version Date: 20080702
Effective Date: 20080707
Expiration Date: 20110707
Responsible Office: Office of the Chief Information Officer

Document Change and Review History

Version Number	Summary of Changes	Changes Made/Reviewed By	Date

Table of Contents

1. Introduction	1
1.1 Purpose	1
1.2 Applicable Documents	1
1.3 Contingency Planning Policies	2
1.4 Contingency Planning Guidance Overview	2
1.5 Contingency Planning and Risk Management Process	3
1.6 Contingency Planning and System Development Life Cycle	3
1.7 Contingency Planning Roles and Responsibilities	4
1.7.1 Office of Security and Program Protection (OSPP)	5
1.7.2 Authorizing Official (AO)	5
1.7.3 Information System Owner (ISO)	5
1.7.4 Agency Chief Information Officer (CIO)	5
1.7.5 Senior Agency Information Security Official (SAISO)	5
1.7.6 Center Information Technology Security Manager (ITSM)	6
1.7.7 Information System Security Officer (ISSO)	6
1.7.8 Contingency Planning Coordinator (CPC)	6
1.7.9 Key Contingency Personnel	6
2. Contingency Planning Process	7
2.1 Develop Contingency Planning Policy	7
2.2 Conduct Business Impact Analysis (BIA)	8
2.2.1 Identify Critical Information Technology Resources	8
2.2.2 Identify Disruption Impacts and Allowable Outage Times	8
2.2.3 Develop Recovery Priorities	9
2.3 Identify Preventative Controls	9
2.4 Develop Recovery Strategies	9
2.4.1 Backup Methods	10
2.4.2 Alternate Sites	10
2.4.3 Equipment Replacement	11
2.4.4 Roles and Responsibilities	12
2.4.5 Cost Considerations	12
2.5 Develop Contingency Plan	13
2.5.1 Contingency Plan Template	14
2.6 Conduct Plan Testing, Training, and Exercises	14
2.6.1 Exercise/Test Objectives	16
2.6.2 Test Scope	16
2.7 Conduct Plan Maintenance	17
3. Approval	19
Appendix A. Acronyms	A-1
Appendix B. Business Impact Analysis Template	B-1
Appendix C. Contingency Plan Template	C-1
Appendix D. Example NASA Tabletop Exercise Plan and Written Test	D-1
Appendix E. Structured Walk Through Test (Simulation Testing)	E-1

1. Introduction

This guidance will assist Agency Program Managers and Information System Owners (ISOs) with the development of viable contingency plans to facilitate a timely response to any disruptive or extended interruption to Agency information systems. The information system contingency plans fit into a much broader emergency preparedness environment, which includes organizational and business process continuity and recovery planning.

This document complies with standard practices as recommended by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, *Contingency Planning Guide for Information Technology Systems* and is in accordance with federally-mandated executive decisions, regulations, and directives and with NASA Procedural Requirement (NPR) 2810.1A, *Security of Information Technology*. The procedures and processes are designed to ensure that the Agency's operations and services promptly resume despite interruptions and disruptions, which might not be resolved by employing normal, daily operating procedures.

To reestablish normal business operations, ISOs must ensure that critical information systems can resume normal functions within a reasonable timeframe; therefore, the contingency planning process is focused on minimizing the duration of a serious disruption, facilitating the effective coordination of recovery tasks, and reducing the complexity of the restoration effort.

1.1 Purpose

The purpose of this guidance is to provide ISOs with a guide for developing information system contingency plans and defining the process necessary to develop and maintain contingency capabilities and implement the requirements of NIST SP 800-34 and NPR 2810.1A. The contingency plans must have sufficient detail so recovery procedures can be carried out by any assigned personnel or team. In an emergency, conditions may exist where personnel who are not in technical positions or who are new to technical positions must assume the duties of experienced technical personnel.

1.2 Applicable Documents

This guidance was developed in accordance with the following regulatory mandates, directives, and federal publications:

- Office of Management and Budget (OMB) Circular No. A-130 Revised, *Management of Federal Information Resources*, February 8, 1996, revised November 2000
- Homeland Security Presidential Directive 7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003
- Public Law 107-347, Title III, Federal Information Security Management Act (FISMA) of 2002, November 25, 2002
- Federal Information Processing Standards (FIPS) Publication, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
- NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, December 2001
- NIST 800-53, (Revision 2) *Recommended Security Controls for Federal Information Systems*, December 2007

- NIST 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, July 2008
- NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006
- NPR 2810.1A, *Security of Information Technology*, May 2006
- NASA Information Technology Requirement (NITR) 2810-15, *Contingency Planning*

1.3 Contingency Planning Policies

NPR 2810.1A as amended by NITR 2810-15, addresses contingency planning for all Agency information systems as required by NIST 800-53, *Recommended Security Controls for Federal Information Systems*, as a security control to ensure the availability of information systems during contingency operations. Agency policy states the following:

- ISOs will develop contingency plans for information systems under their purview in accordance with NIST SP 800-34. For information systems designated Mission Essential Infrastructure (MEI) or are an integral part of a designated MEI, System Owners will coordinate with the Program Office responsible for the Continuity of Operations Plan (COOP).
- ISO's are responsible for ensuring that contingency plans are developed, maintained, and tested in accordance with NITR 2810-15, *Contingency Planning*
- All Agency information systems shall have tested contingency plans
- All Contingency Planning (CP) security controls, including the test/exercise of the system's Contingency Plan, shall be assessed annually
- The Agency Contingency Plan Test Strategy described in NITR 2810-15 shall be used for Contingency Plan exercise and testing

1.4 Contingency Planning Guidance Overview

There are seven major steps in the Agency's contingency planning process, which is aligned with NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*:

- **Develop Contingency Planning Policy** to include the identification of existing requirements, associated plans, programs, and management support.
- **Conduct Business Impact Analysis (BIA)** to identify critical information system functions and resources.
- **Identify Preventive Controls** implemented to reduce the effects of system maintenance (e.g., uninterruptible power supplies (UPS), gas-or diesel-powered generators, smoke detectors, fire suppressors, and water sensors).
- **Develop Recovery Strategies** to include contract agreements, equipment agreements, roles, and responsibilities.
- **Develop Contingency Plan** to restore backup tapes and recover information systems with detailed guidance and procedures.
- **Conduct Plan Testing, Training, and Exercises** to include the development and implementation of regularly scheduled personnel training and testing programs for each information system.

- **Conduct Plan Maintenance** to regularly review and update the plan, control plan distribution, and document plan changes.

These steps will be discussed in Section 2 of this document

1.5 Contingency Planning and Risk Management Process

Risk management activities from the contingency planning perspective have two primary functions. First, risk management should identify threats and vulnerabilities so appropriate controls can be put into place to either prevent incidents from happening or to limit the effects of an incident. These security controls protect an information system against three categories of threats:

- **Natural**—hurricanes, tornados, floods, or fires
- **Human**—operator error, sabotage, malicious code implant, and terrorist attacks
- **Environmental**—equipment failure, software error, telecommunications network outage, and electric power failures

Second, risk management should identify risks for which contingency plans must be put into place. The contingency plan, therefore, is closely tied to the results of the risk assessment and its mitigation process. To effectively determine the specific risks to an information system during service interruption, a risk assessment of the information system environment is required. Since risks can vary over time and new risks may replace old ones as a system evolves, the risk management process must be ongoing and dynamic. The ISO must be aware of system risks and determine whether the current contingency plan addresses risks completely and effectively.

Security categories are used in conjunction with vulnerability and threat information in assessing the risk to an organization. FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* defines the requirement to categorize federal information systems. This categorization is based on the potential impact to an organization should certain events occur that jeopardize their information and information systems, which are needed to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. The system category of low, moderate, or high determines the security controls that must be implemented for the information system, which includes contingency planning controls. The contingency planning controls determine the degree of rigor necessary to prepare the contingency plan; coordinate the plan with other Agency organizations; and determine the frequency of system backups, types of alternate sites selected, training type and frequency, testing type and frequency, and recovery procedure requirements. The risk assessment process facilitates the tailoring of security controls to address organizational needs and risk tolerance.

1.6 Contingency Planning and System Development Life Cycle

System Development Life Cycle (SDLC) refers to the full scope of activities conducted by ISOs who are associated with a system during its life span. The life cycle begins with the project initiation phase and ends with the system disposal phase. Contingency measures should be identified and integrated into all phases of the life cycle—an approach that reduces overall contingency planning costs, enhances contingency capabilities, and reduces the impacts to

system operations if the contingency plan is implemented. Contingency Planning considerations during the SDLC phases are as follows:

- **Initiation Phase.** Contingency planning requirements should be considered when a new information system is being conceived. In the initiation phase, system requirements are identified and matched to their operational processes. Initial contingency requirements may become apparent. During this phase, the new information system shall be evaluated against all other existing and planned information systems to determine its appropriate recovery priority.
- **Development/Acquisition Phase.** As initial concepts evolve into system designs, specific contingency solutions may be incorporated. Contingency measures should continue to reflect system and operational requirements. The design should incorporate redundancy and robustness directly into the system architecture to optimize reliability, maintainability, and availability during the operations/maintenance phase. Backup procedures and timeframes are also defined in this phase. By including these in the initial design, costs, as well as problems associated with retrofitting or modifying the system during later phases, are reduced.
- **Implementation Phase.** While the system is undergoing initial testing, contingency strategies should be tested to ensure that the technical features and recovery procedures are accurate and effective.
- **Operation/Maintenance Phase.** When the system is operational, users, administrators, and managers should maintain a training and awareness program that covers contingency plan procedures. Exercises and tests should be conducted to ensure the procedures remain effective. Regular backups should be conducted and stored offsite. The plan should be updated to reflect changes to procedures based on lessons learned. When the information system undergoes upgrades or any other modifications (e.g., changes to external interfaces), these modifications should be reflected in the contingency plan. Coordinating and documenting changes in the plan should be performed in a timely manner to maintain an effective plan.
- **Disposal Phase.** Contingency considerations should not be neglected because a computer system is retired and another system replaces it. As legacy systems are replaced, they may provide a valuable backup capability if a loss or failure of the new system should occur. In some cases, equipment parts (e.g., hard drives, power supplies, memory chips, or network cards) from hardware that has been replaced by new systems can be used as spare parts for new, operational equipment. In addition, 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.

During the disposal phase, regulatory requirements for data availability must be considered. Though a system has been replaced, it may be necessary to maintain the data, software, or a mechanism to retrieve the data if the historical data is not incorporated into the replacement system.

1.7 Contingency Planning Roles and Responsibilities

This section focuses on contingency planning roles and responsibilities for individuals and organizations; however, it should be noted that these individuals and organizations often have additional responsibilities. Specific responsibilities for each of the NIST 800-53 Contingency Planning security controls is described in NITR 2810-15, *Contingency Planning*.

1.7.1 Office of Security and Program Protection (OSPP)

The Office of Security and Program Protection (OSPP) is responsible for the physical and environmental security controls that protect the Agency information system assets. This responsibility includes facility security and access, Continuity of Operations Plan (COOP) requirements, and personnel security clearance management.

1.7.2 Authorizing Official (AO)

The AO (or Authorizing Official Designated Representative (AODR) in accordance with NIST 800-37) has the authority to formally assume responsibility for operating an information system at an acceptable level of risk to Agency operations (including mission, functions, image, or reputation), Agency assets, or individuals. This includes the contingency planning, including the contingency plan, meeting an acceptable level of risk as part of the system accreditation and the decision for awarding an Approval to Operate. The AO may appoint in writing a Contingency Plan Coordinator (CPC) for specific individual or multiple systems for which they have AO responsibility and may be requested to assist in obtaining resources to develop, implement, maintain, and test/exercise contingency plans.

1.7.3 Information System Owner (ISO)

The Agency is dependent on the ISO to fulfill the business requirements necessary to achieve their program area's mission. The ISOs are responsible for the successful operation of those systems and ultimately accountable for the security of their information systems. They are also responsible for executing crucial steps to achieve management and operational controls and to ensure that appropriate technical controls are effective in protecting the information and information systems under their purview. The ISOs are responsible for ensuring that contingency plans are prepared and coordinated with other Agency offices/organizations, key contingency personnel receive the training required to fulfill their responsibilities, the contingency plan is tested annually, and the plan is maintained and updated when modifications are made to the system.

1.7.4 Agency Chief Information Officer (CIO)

The Agency CIO has the ultimate responsibility to ensure that the Agency has appropriate, tested contingency plans in place to continue fulfilling its mission. During a major disaster or disruption of service, the Agency CIO has the authority to activate the Agency Disaster Recovery Plan (DRP) and initiate the activation of individual system contingency plans. For Center information systems, this authority is delegated to the Center CIOs.

1.7.5 Senior Agency Information Security Official (SAISO)

The SAISO directs the management of the Agency's Information Technology (IT) Security program and develops policies and procedures including contingency planning. The SAISO and the Center Information Technology Security Manager (ITSM) establish a strong foundation in providing oversight to all IT security activities, including contingency planning requirements. The SAISO interacts with internal and external resources, and coordinates security compliance across Agency Centers and other organizational elements.

1.7.6 Center Information Technology Security Manager (ITSM)

The Center ITSM issues IT security policy, procedures, and guidance for all Center information systems. The Center ITSM is responsible for providing oversight to ensure Agency and Center policies are implemented. The ITSM reviews and approves the processes, techniques, and methodologies planned for securing Center information system assets, including contingency planning.

1.7.7 Information System Security Officer (ISSO)

The Information System Security Officer (ISSO) is responsible for ensuring that management, operational, and technical controls for securing Program Office information systems are in place and effective. The ISSO is the principal Point of Contact (POC) for information systems security and is responsible for all security aspects of assigned systems from inception until disposal, including contingency planning.

1.7.8 Contingency Planning Coordinator (CPC)

The Contingency Planning Coordinator (CPC) is appointed in writing by the ISO or the Authorizing Official (AO) to coordinate contingency planning activities for an individual system or multiple systems within the Program Office. The CPC may be the ISO. The ISO retains the responsibility to assure the accomplishment, quality, and implementation of the contingency planning and contingency planning activities. (Note: In the designation ISO actions in this Contingency Planning Guidance, except for approval actions, these responsibilities may be delegated to the CPC) The CPC is responsible for carrying out duties as assigned by the ISO which may include:

- Developing the strategy in cooperation with the functional and resource managers.
- Preparing the Business Impact Analysis
- Developing the Contingency Plan for the ISO in conjunction with senior managers within the Program Office, as well as other Agency offices and organizations
- Coordinating training for individuals with key contingency roles
- Testing the contingency plan, and maintaining the plan
- Distributing the contingency plan to all relevant individuals and organizations according to a list of authorized individuals/organizations
- Directing contingency personnel or teams responsible for the information system(s) and coordinating their actions with other relevant Agency personnel or organizations when the contingency plan is executed.

1.7.9 Key Contingency Personnel

Contingency personnel are responsible for the execution and implementation of activities as specified in the information system contingency plan.

2. Contingency Planning Process

This section provides guidance on developing, testing, and maintaining information system contingency plans. Ultimately, the Agency, individual Program Offices and ISOs will have a suite of plans to prepare proper response, recovery, and continuity activities for disruptions affecting Agency information systems, business processes, and facilities. Because there is an inherent relationship between an information system and the business process it supports, there must be coordination between each plan during development and updates to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts.

The Business Continuity Plan (BCP) focuses on sustaining an organization's business functions during and after a disruption (e.g., payroll process or consumer information process). A BCP may be written for a specific business process or may address all key business processes. The BCP considers information systems in terms of their support to business processes. In some cases, the BCP may not address long-term recovery and return to normal operations, but solely cover interim business continuity requirements. To eliminate possible conflicts, the responsibilities and priorities set in the BCP must be coordinated with those responsible for Continuity Of Operations (COOP) Planning Procedural Requirements (NPR) 1040.1. Most Agency designated Mission Essential Infrastructure (MEI) systems will include a formal COOP. This coordination is particularly critical if the information system is a designated MEI or an integral element of a designated MEI.

The COOP focuses on restoring an organization's essential functions at an alternate site and performing mission critical functions for up to 30 days before these functions return to normal operations. The COOP usually addresses Agency issues and is developed and executed independently from the BCP. Because the COOP emphasizes the recovery of an organization's operational capability at an alternate site, the plan does not necessarily include IT operations. In addition, the plan does not typically address minor disruptions that do not require relocation to an alternate site.

The DRP applies to major, usually catastrophic, events that deny access to the normal facility for an extended period. Frequently, DRP refers to an IT-focused plan designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency. The DRP scope may overlap that of an information system contingency plan; however, the DRP is narrower in scope and does not address minor disruptions that do not require relocation.

Information systems are vital elements in most business processes. Because business process resources are essential to an organization's success, it is critical that the services provided by these systems can operate effectively without excessive interruption. The information system contingency plan supports this process by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered quickly and effectively following a service disruption or disaster. Because an information system contingency plan should be developed for each major application and general support system, multiple contingency plans may be maintained within the organization's BCP.

2.1 Develop Contingency Planning Policy

The development and maintenance of the Agency contingency planning policy and contingency planning guidance is the responsibility of the SAISO. The Agency's contingency planning policy

was developed and is addressed in NPR 2810.1A as amended by NITR 2810-15, *Contingency Planning*. According to the policy, the ISOs have the responsibility for developing, testing and maintaining contingency plans for the systems under their purview. This document provides guidance to ISOs on how to implement Agency contingency planning requirements as defined in the NPR 2810.1A and NITR-2810-15. This guidance must be implemented in coordination with related Agency activities (e.g., physical security, human resources, IT operations, and emergency preparedness functions). Contingency planning personnel must coordinate activities from each area to remain aware of new or evolving policies, programs, or capabilities.

2.2 Conduct Business Impact Analysis (BIA)

The BIA is a key step in the contingency planning process that collects the information to fully characterize system requirements, processes, and interdependencies. The BIA template is in Appendix B. This information is used to determine contingency requirements and priorities. The purpose of the BIA is to correlate specific system components with the critical services they provide and, based on that information, characterize the consequences of a disruption to system components. Results from the BIA are incorporated into the analysis and strategy development efforts for the information system contingency plan and will be included in the contingency plan as an appendix.

The BIA should be reviewed periodically and updated with new information to identify new contingency requirements or priorities. As new technologies become available, preventive measures may be enhanced and recovery strategies may be modified.

2.2.1 Identify Critical Information Technology Resources

The first step in the BIA is to evaluate the information system to determine critical functions performed by the system and to identify the specific system resources required to perform them. Two activities that are required by this step include:

- Identify and coordinate with internal and external points of contact (POC) associated with the system to characterize the ways POCs depend upon or support the information system. When identifying contacts, it is important to include organizations that provide or receive information from the system, as well as contacts supporting any interconnected systems. This coordination should enable the ISO to characterize the full-range of support provided by the system.
- Evaluate the system to link these critical services to system resources. This analysis usually will identify infrastructure requirements, such as electric power, telecommunication connections, and environmental controls. Specific equipment (e.g., routers, application servers, and authentication servers) is usually considered critical; however, the analysis may determine that certain components (e.g., printer or print server) are not needed to support critical services.

2.2.2 Identify Disruption Impacts and Allowable Outage Times

Once critical information system resources have been evaluated, the ISO should analyze these resources and determine what the impact on information system operations would be if a given resource were disrupted or damaged. The ISO must determine how long a disruption of service is acceptable based on the impact the outage has on accomplishing the Agency's mission. The

ISO shall balance the cost of system inoperability against the cost of resources required to restore the system. The analysis should evaluate the impact of the outage in two ways:

- The effects of the outage may be tracked over time. This enables the ISO to identify the maximum allowable time that a resource may be denied before it prevents or inhibits the performance of an essential function.
- The effects of the outage may be tracked across related resources and dependent systems, identifying any cascading effects that may occur as a disrupted system affects other processes that rely on it.

2.2.3 Develop Recovery Priorities

The outage impacts and allowable outage times characterized in the previous step enable the ISO to develop and prioritize recovery strategies that personnel will implement during contingency plan activation. For example, if the ISO determines that the system must be recovered within 24 hours, measures to meet the requirement and obtain the necessary resources to accomplish the recovery goals must be determined. By prioritizing these recovery strategies, the ISO may make more informed, tailored recommendations regarding contingency resource allocations and expenditures, as well as save time, effort, and cost. Implementing recovery strategies usually requires coordinating with other Agency organizations.

2.3 Identify Preventative Controls

The outage impacts identified in the BIA may be mitigated or eliminated through preventive measures that deter, detect, 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. A wide variety of preventive controls are available, depending on system type and configuration. Some common measures include:

- Fire suppression systems
- Fire and smoke detectors
- Plastic tarps that may be unrolled over equipment to protect it from water damage
- Offsite storage of backup media, non-electronic records, and system documentation
- Appropriately sized UPS

Preventive controls should be documented in the contingency plan and personnel associated with the system should be trained on how and when to use the controls. These controls should be maintained in good condition to ensure their effectiveness in an emergency.

2.4 Develop Recovery Strategies

Recovery strategies provide a means to restore information system 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 strategy, including cost, allowable outage time, security, and integration with larger, organization-level recovery plans.

The selected recovery strategy should address the potential impacts identified in the BIA and be integrated into the system architecture during the design and implementation phases of the information system life cycle. The strategy should include a combination of methods that complement each other to provide recovery capability over the full spectrum of incidents. A wide variety of recovery approaches may be considered, with the appropriate choice dependent on the incident, type of system, and its operational requirements. When developing a system recovery strategy, specific recovery methods may include commercial contracts with cold, warm, hot, mobile, or mirrored sites; reciprocal agreements with internal or external technologies (e.g., Redundant Arrays of Independent Disks (RAID); automatic fail-over, UPS, and mirrored systems).

2.4.1 Backup Methods

In order to support events requiring the recovery of information systems, the information system backups to recover the system must be stored at an alternate site. Backup frequency should be based on Agency policy, data criticality, and the frequency that new information is introduced. The location of stored data, file-naming conventions, media rotation frequency, and method for transporting data offsite should be documented in the contingency plan. The specific method selected for conducting backups should be based on system and data availability and integrity requirements. When the data is required for recovery or testing purposes, the organization contacts the storage facility requesting that the specific data be transported to the organization or to an alternate facility.

2.4.2 Alternate Sites

Although major disruptions with long-term effects may be rare, they should be documented in the contingency plan. The plan must include a strategy to recover and perform system operations at an alternate facility for an extended period. The alternate site facility must be able to support system operations as defined in the contingency plan. The three alternate site types may be categorized in terms of their operational readiness. Sites may be identified as cold, warm, hot, mobile, or mirrored. Progressing from basic to advanced, the five types of sites are described as follows:

- **Cold Sites**—typically consist of a facility with adequate space and infrastructure (e.g., electric power, telecommunications connections, and environmental controls) to support the information system. The space may have raised floors and other attributes suited for information system operations. The site does not contain equipment and usually does not contain office automation equipment (e.g., telephones, facsimile machines, or copiers). The organization using the cold site is responsible for providing and installing necessary equipment and telecommunications capabilities.
- **Warm Sites**—partially equipped office spaces that contain some or all system hardware, software, telecommunications, and power sources. The warm site is maintained in an operational status ready to receive the relocated system. The system may need preparation before receiving the system and recovery personnel. In many cases, a warm site may serve as a normal, operational facility for another system or function, and in the event of contingency plan activation, the normal activities are displaced temporarily to accommodate the disrupted system.
- **Hot Sites**—office spaces appropriately sized to support system requirements and configured with 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 preparations for system arrival as soon as they are notified that the contingency plan has been activated.

- **Mobile Sites**—self-contained, transportable shells that are custom-filled with specific telecommunications and information system equipment necessary to meet system requirements. The facility is often contained in a tractor-trailer and may be driven to and set up 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 a Service Level Agreement (SLA) should be signed between the two parties.
- **Mirrored Sites**—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.

There are many cost and ready-time differences among the five options. The mirrored site is the most expensive choice; but it ensures virtually 100 percent availability. Cold sites are the least expensive to maintain; however, they may require substantial time to acquire and install the necessary equipment. Partially equipped sites (e.g., warm sites) fall in the middle of the spectrum. In many cases, mobile sites may be delivered to the desired location within 24 hours. The selection of the fixed site locations should account for the time and mode of transportation necessary to move personnel to the site. In addition, the fixed site should be in a geographic area that is unlikely to be negatively affected by the same disaster event as the organization's primary site. As the sites are evaluated, the ISO should ensure that the system's security, management, and operational and technical controls are compatible with the prospective site. Such controls may include firewalls and physical access controls, data remnance controls, and security clearance level of the site and personnel supporting the site.

2.4.3 Equipment Replacement

If the information system is damaged or destroyed or the primary site is unavailable, necessary hardware and software must be activated or procured quickly and delivered to the alternate location. Three basic strategies exist to prepare for equipment replacement. 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. The three basic strategies are described as follows:

- **Vendor Agreements**—as the contingency plan is being developed, SLAs for hardware, software, and support vendors may be made for emergency maintenance service. The SLA should specify how quickly the vendor must respond after being notified. The agreement should also give the organization's priority status for the shipment of replacement equipment over equipment being purchased for normal operations. SLAs should further discuss what priority status the organization will receive in the event of a catastrophic disaster involving multiple vendor clients. In such cases, organizations with health- and safety-dependent processes will often receive the highest priority for shipment. The details of these negotiations should be documented in the SLA, which should be maintained with the contingency plan.
- **Equipment Inventory**—required equipment may be purchased in advance and stored at a secure offsite location, such as an alternate site where recovery operations will take place (i.e., warm or mobile site) or at another location where it will be stored and then shipped to the alternate site. This solution has certain drawbacks since the 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.

- **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.

When evaluating the choices, the ISO should consider that purchasing equipment when needed is cost-effective, but can add significant overhead time to the recovery process while waiting for shipment and setup. Conversely, storing unused equipment is costly, but allows recovery operations to begin more quickly. Based on the impacts discovered through the risk management process and BIA, consideration should be given to the possibility of a widespread disaster requiring mass equipment replacement and transportation delays that would extend the recovery period. Regardless of the strategy selected, detailed lists of equipment needs and specifications should be maintained within the contingency plan.

2.4.4 Roles and Responsibilities

Having selected and implemented the system recovery strategy, the ISO must designate appropriate personnel or teams to implement the system recovery strategy. Each individual should be trained and ready to deploy in the event of a disruptive situation requiring plan activation. Recovery personnel should be assigned to one of several specific teams who will respond to the event, recovery capabilities, and return the system to normal operations. To accomplish this, they need a clear understanding of the team's goal in the recovery effort, each step they are to execute, and how their team relates to other teams.

Personnel should be chosen to staff these teams based on their skills and knowledge. Ideally, teams would be staffed with the personnel responsible for the same or similar operation under normal conditions. Team members must not only understand the contingency plan's purpose, but also need to know the procedures necessary to execute the recovery strategy. Teams should be sufficient in size to remain viable if some members are unavailable to respond or alternate team members may be designated. Similarly, team members should be familiar with the goals and procedures of other teams to facilitate inter-team coordination. The ISO should also consider that a disaster could occur that would render a majority or all personnel unavailable to respond. In this situation, executing the plan may only be possible by using personnel from another geographic area of the organization or by hiring contractors or vendors. Such personnel may be coordinated and trained as an alternate team.

Each team is led by a team leader who directs overall team operations and acts as the team's representative to management and liaisons with other team leaders. The team leader disseminates information to team members and approves any decisions that must be made within the team. Team leaders should have a designated alternate to act as leader if the primary leader is unavailable.

2.4.5 Cost Considerations

The ISOs must ensure that the strategy chosen can be implemented effectively with available personnel and financial resources. The cost of each type of alternate site, equipment replacement, and storage option under consideration should be weighed against budget

limitations. The ISO should determine known contingency planning expenses (e.g., alternate site contract fees) and those less obvious (e.g., cost of implementing an agency-wide contingency awareness program and contractor support). The budget must be sufficient to encompass software, hardware, travel, shipping, testing, plan training programs, awareness programs, labor hours, other contracted services, and any other applicable resources (e.g., desks, telephones, fax machines, pens, and paper). The Program Office should perform a Cost Benefit Analysis (CBA) to identify the optimum recovery strategy.

2.5 Develop Contingency Plan

Documenting information in the contingency plan is a critical step in the process of implementing a comprehensive Contingency Planning Program. The plan should contain detailed roles and responsibilities and procedures associated with restoring the information system following a disruption. The contingency plan documents the technical capabilities designed to support contingency operations and is tailored to the organization and its requirements.

Contingency plans should be formatted to provide quick and clear directions in the event that personnel not familiar with the plan or the systems can be called upon to perform recovery operations. Plans should be clear, concise, and easy to implement in an emergency. Where possible, checklists and step-by-step procedures should be used. A concise and well-formatted plan reduces the likelihood of unnecessary complexity and confusion at the time of implementation. There are five main components of the contingency plan:

- **Supporting Information.** This section includes an Introduction and Concept of Operations (CONOPS) section providing essential background or contextual information that makes the contingency plan easier to understand, implement, and maintain. This information assists in making decision on how to use the plan and provides information on where associate plans and information outside the scope of the plan may be found. The Introduction section orients the reader to the type and location of information contained in the plan. The CONOPS provides additional details about the information system and contingency planning framework, as well as response, recovery, and resumption activities.
- **Notification/Activation.** This section defines the initial actions taken once a system disruption or emergency has been detected or appears to be imminent. It defines activities to notify personnel, assess system damage, and implement the plan. The notification/activation section also defines the personnel necessary to complete these tasks.
- **Recovery.** This section documents the activities that take place after the plan has been activated, damaged assessed, personnel notified, and teams mobilized. It focuses on contingency measures to execute temporary information system processing capabilities, repair damage to the original system, and restore operational capabilities at the original or new facility. This section documents information on temporary manual processing plans, recovery and operational procedures at an alternate system, or relocation and recovery procedures at an alternate site.
- **Reconstitution.** This section of the contingency plan focuses on activities after recovery activities are terminated and normal operations are transferred back to the organization's original facility. If the original facility is unrecoverable, the procedures can be used to prepare a new facility to support information system processing requirements.

- **Plan Appendices.** The contingency plan appendices provide key details that are not contained in the main body of the plan and that reflect specific technical, operational, and management contingency system requirements. However, some contingency plan appendices are frequently found with contingency plans. Common contingency appendices include the following information:
 - Contact information for contingency planning team personnel
 - Vendor contact information, including offsite storage and alternate site POCs
 - Standard operating procedures (SOP) and checklists for system recovery or processes
 - Equipment and system requirements lists of hardware, software, firmware, and other resources required to support system operations
 - Vendor SLAs, reciprocal agreements with other organizations, and other vital records
 - Descriptions of, and directions to, the alternate site
- BIA

2.5.1 Contingency Plan Template

The contingency plan template is provided as Appendix C and includes the templates needed for the Contingency Plan completion and approval.

2.6 Conduct Plan Testing, Training, and Exercises

Contingency plan testing is a critical element of a viable contingency capability and is required annually in accordance with NIST 800-53, *Recommended Security Controls for Federal Information Systems*. Testing enables plan deficiencies to be identified and addressed. Testing also helps evaluate the ability of recovery personnel to implement the plan quickly and effectively. Each contingency plan element shall be tested to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan. The following areas shall be addressed in the contingency test:

- System recovery on an alternate platform from the backup media
- Coordination among Recovery Teams
- Internal and external connectivity
- System performance using alternate equipment
- Restoration of normal operations
- Notification procedures

The Agency's security policy states that testing for all systems shall be done annually (fiscal year). The contingency plan testing should be done at approximately the same time each year, but completed no later than July 31st. If major changes have been made to the system, the contingency plan should be updated, distributed, and tested prior to implementation.

Participants in the exercises and tests should include key personnel identified in the contingency plan, operational personnel, recovery and restoration personnel and the ISO.

To derive the most value from the test, the ISO should develop a test plan designed to test the selected elements against explicit test objectives and success criteria. The test plan should

include a schedule detailing the timeframes for each test and test participants. The test plan should also delineate clear scope, scenario, and logistics. The scenario chosen may be a worst-case incident or an incident that is most likely to occur.

There are two basic formats for exercises:

- **Classroom Exercises/Tabletop Test.** Participants in the classroom exercises, often called tabletop exercises, walk through the procedures without any actual recovery operations occurring. Classroom exercises are the most basic and least costly of the two types of exercises and should be conducted before performing a functional exercise. It is designed to test the knowledge and awareness of the teams and to ensure that participants are aware of their roles and participation in the processes to recover data and systems. A written test can be a useful component of the classroom exercise allowing the Test Leader to obtain information from geographically and organizationally diverse groups. A sample tabletop test is included in Appendix D.
- **Functional Exercises.** Functional exercises are more extensive than tabletops, requiring an event to be replicated. Functional exercises include simulations and war-gaming. Often, scripts are written out for role players pretending to be external organization contacts, or there may be actual interagency and vendor participation.
 - **Functional Exercises/Simulation Exercise.** This is a more advanced test. A simulation exercise uses the existing contingency plan and measures its effectiveness against a fictional series of catastrophic events. All responsible staff should be present at the simulation, as well as a representative from each business unit. This exercise may be an integrated test that includes all system interfaces and related systems. A sample Simulation Exercise is included as Appendix E.
 - **Functional Exercises/Alternate Site Test.** This test transfers operations to the alternate restoration facility and is used to ensure that the alternate site operates as planned during the recovery process and after the system has been recovered. Third-party vendors may be included in this test. This exercise may be an integrated test that includes all system interfaces and related systems.

Announcing the plan in advance is a benefit to team members so they can prepare for it mentally and prioritize their workload. It is likely that some team members will not be available. This itself is beneficial to the plan test to capture how a real response may play out, providing critical input to improve the plan. It is important that an exercise should not disrupt normal operations. If testing at the alternate facility, the ISO should coordinate test dates and operations with the Manager of the alternate facility.

Test results and lessons learned shall be documented in the RMS C&A Documentation Repository and POA&M Management System, referred to as RMS, and reviewed by test participants and other personnel, as appropriate. Information collected during the test and post-test reviews that improve plan effectiveness shall be incorporated into the contingency plan. The test results shall be submitted to the Center ITSM and the ISO.

Training for personnel with contingency plan responsibilities should complement testing. Training should be provided at least annually and new personnel who will have contingency plan responsibilities should receive training shortly after being assigned those responsibilities. Ultimately, contingency plan 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:

- Purpose
- Cross-team coordination and communications
- Reporting procedures
- Security requirements
- Team-specific processes
- Individual responsibilities

2.6.1 Exercise/Test Objectives

Test objectives must be clearly defined prior to the initiation of the contingency plan test or exercise. Each individual or team, as defined in the contingency plan, must anticipate the sequence of events leading to a system resumption or recovery and know their precise individual role and responsibility to support an effective recovery effort.

All contingency plan tests should meet the following objectives:

- Verify that all individuals and team members understand their role in the resumption or recovery of a system.
- Resolve all questions and ambiguities during the exercise/test.
- Provide the Agency's management and team leads with a test summary prepared by the test moderator outlining successes and areas for improvement.
- Initiate improvements to the contingency plan based on discussions, observations, and findings identified during the test.

In addition to the above objectives, functional/simulation exercises include the following objectives:

- Validate assumptions and dependencies as documented in the plan.
- Conduct simulation of activities as documented in the plan to include restoration, system and integrated testing.

The functional exercises/alternate site testing includes the following additional objectives:

- Conduct network and communication restoration activities.
- Determine actual recovery timeframes for required components.
- Note ambiguities in the plan and actions taken to resolve them.
- Determine need and schedule for future alternate site tests based on the results and the system impact categorization.

2.6.2 Test Scope

The scope of the contingency plan test or exercise must be documented during the planning stages. The scope of the contingency plan test may include testing the recovery plan or

resumption of the general support systems, the communications and network connections, specific systems and/or all systems interfaces.

The classroom exercises/tabletop tests and functional/simulation exercises consist of written and verbal acknowledgement by team members of their recovery and restoration responsibilities, as well as a demonstration of their knowledge of the recovery process and their specific duties within the process. These types of tests/exercises are limited to questions and answers, and discussions. For the classroom exercises/tabletop tests or the simulation exercises the scope does not include any hands-on use of equipment that is used during an actual recovery (e.g., phone system, tape backup unit, server, router) and does not include a walk-through of the alternate relocation site.

The functional exercise/alternate site test includes hands-on use of equipment for the actual recovery of the system to include backup media and required hardware and software components. The scope may include recovery of all operating systems necessary for the systems being tested, as well as communications and network components, system interfaces, and system inputs and outputs at the site may be tested. In addition, the recovery time objectives for all components are tested.

2.7 Conduct Plan Maintenance

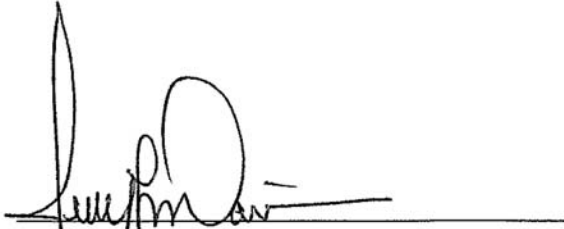
The contingency plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. Information systems frequently change due to shift of business needs, technology upgrades, or new internal or external policies. Therefore, it is essential that the contingency plan be reviewed and updated regularly as part of the organization's change management process to ensure that new information is documented and contingency measures revised, if required. NITR 2810-15 requires ISOs to review the contingency plans for accuracy and completeness at least annually or whenever significant changes occur to any element of the plan. Certain elements will require more frequent reviews, such as contact lists. Based on the system type and criticality, it may be necessary to evaluate contingency plan content and procedures more frequently. At a minimum, plan reviews should focus on the following elements:

- Operational requirements
- Security requirements
- Technical procedures
- Hardware, software, and other equipment (e.g., types, specifications, and amount)
- Team members names and contact information
- Alternate and offsite facility requirements
- Vital records (e.g., electronic and hardcopy)

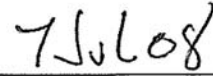
Because the contingency plan contains sensitive operational and personnel information, its distribution should be marked accordingly and controlled. Typically, copies of the plan are provided to recovery personnel for storage at home and office. Additionally, a copy should also be stored at the alternate site in the event local plan copies cannot be accessed because of the disaster. Other information that should be stored with the contingency plan include contracts with vendors (e.g., SLAs and other contracts), software licenses, system user manuals, security manuals, and operating procedures.

The ISO should work closely with associated internal and external organizations and system POCs to ensure that impacts caused by changes within interconnected organizations will be reflected in the contingency plan.

3. Approval



Jerry L. Davis
Deputy CIO IT Security
Senior Agency Information Security Officer



Date

Appendix A: Acronym

AO	Authorizing Official
AODR	Authorizing Official Designated Representative
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CBA	Cost Benefit Analysis
CIO	Chief Information Officer
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan
CP	Contingency Plan
CPC	Contingency Plan Coordinator
DRP	Disaster Recovery Plan
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
HSPD	Homeland Security Presidential Directive
ISO	Information System Owner
ISSO	Information System Security Officer
IT	Information Technology
ITSM	Information Technology Security Manager
MEI	Mission Essential Infrastructure
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NITR	NASA Information Technology Requirement
NPD	NASA Procedural Directive
NPR	NASA Procedural Requirements
OMB	Office of Management and Budget
OSPP	Office of Security and Program Protection
POC	Point of Contact
RAID	Redundant Arrays of Independent Disks
RMS	Risk Management System C&A Documentation Repository and POA&M Management System
SAISO	Senior Agency Information Security Official
SDLC	System Development Life Cycle

SLA	Service Level Agreement
SOP	Standard Operating Procedures
SP	Special Publication
UPS	Uninterruptible Power Supply

Appendix B: Business Impact Analysis Template

Business/Mission Impact Analysis

[System Name]

Organization		Date BIA Completed		Confidentiality	Integrity	Availability	System Criticality as defined by FIPS:
		BIA POC					Moderate

System Description

Recovery Priority	Critical Resource / Function	Critical Role and Department	Maximum Allowable Outage	Business Impact	
				Impact	Comments
<p>List the priority associated with recovering a specific resource, based on the outage impacts and allowable outage times.</p>	<p>Identify the specific hardware, software, and other resources (include system dependencies and interdependencies) that comprise the system; include quantity and type.</p>	<p>Identify the individuals, positions, offices, agencies or organizations that supports the system; also specify their relationship to the system.</p>	<p>Identify the maximum acceptable period that the resource could be unavailable before unacceptable impacts resulted.</p>	<p>Based on the outage impacts and allowable outage times provided. Use quantitative or qualitative scale (e.g., high/moderate/low).</p> <p>High Mod Low</p>	<p>Describe the business impact on mission if the critical resource is unavailable.</p>
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					

Appendix C: Contingency Plan Template

This template is provided to assist ISOs in preparing a contingency plan for their information systems. Where practical, the template provides instructions for completing specific sections and text is added in certain sections. However, the information is intended only to suggest the type of information that may be found in that section. The text is not comprehensive and should be modified to meet specific system considerations. While the template provides a standard approach for all Agency contingency plans, ISOs may modify the template slightly to best accommodate their specific system.

Instructions on Completing the Template

- Texts in Blue are either instruction texts or text that needs to be deleted and filled in by the writer of the plan.
- Texts in Black are standard template text that are required to be included in the Contingency Plan and should not be deleted unless necessary.
- Instructions for each section are included in each Discussion Box on how to complete and fulfill the requirements for that section. Discussion Boxes can be deleted after the section has been completed or may be left there for future reference.
- Examples are given within each section. It is advised that the examples are deleted after the section has been completed to prevent any reader confusion.



Contingency Plan Template

[SYSTEM NAME]

[SSP Number]

[Organization]

[DATE PREPARED]

Prepared by:

Preparing Organization

Contingency Plan Template V1.0, June 2008

REVIEW AND APPROVAL SIGNATURES

This Contingency Plan for the [SYSTEM NAME] was prepared for the exclusive use of the [AGENCY].

Reviewed by: _____
Information System Security Officer Date

I have reviewed and concur with the contents of this plan.

Approved by: _____
Information System Owner Date

Approved by: _____
ITSM (or Designated Representative) Date

Document Change and Review History

Version Number	Summary of Changes	Changes Made/Reviewed By	Date

TABLE OF CONTENTS

1. Introduction	6
1.1 Purpose	7
1.2 Applicability	8
1.3 Planning Principles	8
1.4 Assumptions	8
1.5 Reference/Requirements	9
2. System Identification	10
System Name/Title	10
2.1 Responsible Organization	10
2.2 Information Contact(s) and Line of Succession	10
2.3 Information System Categorization	12
2.4 Mission Criticality	13
2.5 System Description and Architecture	13
2.6 System Interconnection/Information Sharing	13
3. Notification and Activation Phase	15
3.1 Damage Assessment Procedures	15
3.2 The Contingency Plan Activation	15
3.3 Alternate Location Procedures	16
4. Recovery Operations Phase	18
4.1 Recovery Procedures and Objectives	18
5. Reconstitution Phase	20
5.1 Concurrent Processing	20
5.2 Plan Deactivation	20
6. Training, Testing and Exercises	21
6.1 Contingency plan Testing and Exercise	21
6.2 Documenting Test Plan Results	21
6.3 Plan Maintenance	22
Attachment 1: Emergency / Disaster Team Formulation	24
Attachment 2: Damage Assessment Checklist	30
Attachment 3: Contingency Log and Action Item checklist	32
Attachment 4: Contingency Plan Test Strategy	35
Attachment 5: Contingency Plan Test Results	35

1. Introduction

This document contains the Contingency Plan for the *[System Name]*. It is intended to serve as the centralized repository for the information, tasks, and procedures that would be necessary to facilitate the *[System Name]* management's decision-making process and its timely response to any disruptive or extended interruption of the department's normal business operations and services. This is especially important if the cause of the interruption is such that a prompt resumption of operations cannot be accomplished by employing only normal daily operating procedures.

In terms of personnel and financial resources, the information tasks and procedures detailed in this plan represent the *[System Name]* management's demonstrated commitment to response, resumption, recovery, and restoration planning. Therefore, it is essential that the information and action plans in this plan remain viable and be maintained in a state of currency in order to ensure the accuracy of its contents. To that end, this introduction is intended to introduce and familiarize its readers with the organization of the plan.

It is incumbent upon every individual who is in receipt of the *[System Name]* Contingency Plan, or any parts thereof, or who has a role and/or responsibility for any information or materials contained in the document, to ensure that adequate and sufficient attention and resources are committed to the maintenance and security of the document and its contents.

Since the information contained in this document describes *[System Name]* management's planning assumptions and objectives, the plan should be considered a sensitive document. All of the information and material contents of this document should be labeled, "SENSITIVE BUT UNCLASSIFIED (SBU)".

The *[System Name]* management has recognized the potential financial and operational losses associated with service interruptions and the importance of maintaining viable emergency response, resumption, recovery and restoration strategies.

The *[System Name]* Contingency Plan is intended to provide a framework for constructing plans to ensure the safety of employees and the resumption of time-sensitive operations and services in the event of an emergency and/or disaster (fire, power or communications blackout, tornado, hurricane, flood, earthquake, civil disturbance, etc.).

Although the *[System Name]* Contingency Plan provides guidance and documentation upon which to base emergency response, resumption, and recovery planning efforts, it is not intended as a substitute for informed decision-making. Business process managers and executives must identify services for which disruption will result in significant financial and/or operational losses.

Discussion:

Plans should include detailed responsibilities and specific tasks for emergency response activities and business resumption operations based upon pre-defined time frames. Constructing a plan and presenting it to senior management may satisfy the immediate need of having a documented plan. However, this is not enough if the goal is to have a viable response, resumption, recovery, and restoration capability.

A Contingency Plan is not a one-time commitment and is not a project with an established start and end date. Instead, Contingency Plans are an on-going, funded business activity budgeted to provide resources required to:

- Perform activities required to update and create plans
- Train employees on a continuous basis
- Develop and revise policies and standards as the department changes
- Exercise strategies, procedures, team and resources requirements
- Re-exercise unattained exercise objectives
- Report on-going continuity planning to senior management
- Research processes and technologies to improve resumption and recovery efficiency
- Perform plan maintenance activities

This Contingency Plan encompasses activities required to maintain a viable continuity capability and ensures that a consistent planning methodology is applied to **[System Name]**. Contingency Plan elements necessary to create a viable, repeatable and verifiable continuity capability include:

- Implement accurate and continuous vital records, data backup, and off-site storage
- Construct contingency response teams
- Implement contingency strategies

1.1 Purpose

Discussion:

If this is the first time the Contingency Plan has been written, the Contingency Plan Coordinator (CPC) should consult with Information System Owners (ISOs), developers and/or staff concerning information on current Disaster Recovery Planning (DRP).

This **[System Name]** Contingency Plan establishes procedures to recover the **[System Name]** following a disruption. The following objectives have been established for this plan:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
 - Notification/Activation phase
 - Recovery phase
 - Reconstitution phase
- Identify the activities, resources, and procedures needed to carry out **[System Name]** processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated **[Organization Name]** personnel and provide guidance for recovering **[System Name]** during prolonged periods of interruption to normal operations.
- Ensure coordination with other **[Organization Name]** staff that will participate in the contingency planning strategies. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

1.2 Applicability

The *[System Name]* Contingency Plan applies to the functions, operations, and resources necessary to restore and resume *[Organization Name]*'s *[System Name]* operations at *[Primary Location Name]*, *[City]*, *[State]*. The *[System Name]* Contingency Plan applies to all personnel associated with *[System Name]* as identified under Section 2.2.1, Roles and Responsibilities.

The *[System Name]* Contingency Plan is supported by *[Plan Names, i.e., Mission Essential Infrastructure (MEI) COOP, Configuration Documentation, Design Documentation]*, which provides the *[Purpose of the plans]*. Procedures outline in this plan are coordinated with and support the aforementioned documents.

1.3 Planning Principles

This plan does not identify contingencies for every possible scenario. Rather, it focuses on two scenario types: (1) Minor System Failure and (2) Major System Failure. Full Contingency Plan implementation may not be required for all disruptions. In some cases, partial implementation may be appropriate. The *[System Name]* Contingency Plan is based on the following scenarios: The Contingency Plan will not be activated for a Minor System Failure; however, should be considered for full implementation for most Major System Failures. The scenarios are described in more detail below.

Scenario 1 – Minor System Failure

A localized threat has caused a disruption of *[System Name]* services in one or both of the following:

- The application has become inoperable for a period of less than 24 hours and major components of the system are still operational.
- The facility that houses the failed component has not been physically damaged to an extent that requires personnel evacuation or major repair to the environment.

Scenario 2 – Major System Failure

A localized threat has caused a disruption of *[System Name]* services in one or both of the following:

- The application has become inoperable for a period (present or expected) of more than 24 hours.
- The facility that houses the failed components has been physically damaged to an extent that requires temporary personnel evacuation or major repair to the environment.

1.4 Assumptions

Based on these principles, the following assumptions were used when developing the Contingency Plan:

- The NASA Local Area Network/Wide Area Network (LAN/WAN) is operational.
- Key Agency personnel have been identified and trained in their emergency response and recovery roles and are available to activate the Contingency Plan.
- Access to backup data, configuration files, hardware, and software is accessible by key Contingency Plan personnel.
- Service level agreements (SLA) are maintained with system hardware and software vendors to support emergency system recovery.
- The **[System Name]** Contingency Plan is up to date and accessible to key personnel responsible for executing the plan.
- The procedures within the plan have been tested to ensure that the strategies are viable.

Discussion:

Add additional assumptions as necessary.

The **[System Name]** Contingency Plan does not apply to the following situations:

- Overall recovery and continuity of business operations
- Emergency evacuation of personnel
- Detailed procedures for the relocation of IT functions to an alternate site if the original site is damaged.

Discussion:

Add additional situations as necessary.

1.5 Reference/Requirements

The **[System Name]** Contingency Plan also complies with the following federal and departmental policies: **Add in additional departmental policies if needed.**

- *Federal Information Security Management Act of 2002*
- *Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, November 2000.*
- *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Contingency Planning Guide for Information Technology Systems, June 2002.*
- *NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*
- *NIST SP 800-100, Information Security Handbook: A Guide for Managers, October 2006.*
- *NPR 2810.1A, Security of Information Technology (WITH NITR amendments)*

2. System Identification

System Name/Title

Discussion:

Enter the information system name and acronym

2.1 Responsible Organization

Discussion:

In this section, list the organization that owns and is responsible for the data in the application. The responsible organization owns the system, the data it contains, and controls the use of the data. List the federal organizational sub-component responsible for the system. If another federal Agency or contractor performs the function, identify both the federal organization and contractor (if applicable) and describe the relationship. Be specific about the organization and do not abbreviate. Include phone numbers, physical locations, and addresses.

The responsible organization owns the system, the data it contains, and controls the use of the data.

Example:

NASA
300 E St SW
Washington, DC 20410
202-358-1234 x1234

The System is maintained by:

Appropriate Contractor Firm
1234 Main St
Anywhere, USA, 12345
123-456-7890 x0000

2.2 Information Contact(s) and Line of Succession

Discussion:

Specify the program owner, program manager and the system manager to contact for further information regarding the contingency plan and the system. Include their address, telephone number(s), and e-mail. List the name, title, organization, and telephone number of one or more persons designated to be the point(s) of contact for this system. The contacts given should be identified as the ISO, program manager, system manager, and Information System Security Official (ISSO). The designated persons should have sufficient knowledge of the system to be able to provide additional information or points of contact, as needed.

The designated person(s) have sufficient knowledge of the system to be able to provide additional information or points of contact regarding the system, as needed. The [ISO]/[insert position], [Organization Name] is responsible for execution of the contingency procedures documented within the [System Name] Contingency Plan, and for ensuring the safety of personnel. If the [insert name or position] is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the [insert name or position] will assume this responsibility.

Example:

ISO

Jane Roe
Information Resource Management Office
NASA
300 E Street S.W.,
Washington, DC 20410
202-358-1234
ima.pony@nasa.gov

Designated Representative

John Doe
NASA
Office of ABC
300 E Street S.W.,
Washington, DC 20410
202-358-1234
john.doe@nasa.gov

2.2.1 [System Name] Contingency Team Roles and Responsibilities**Discussion:**

Describe each team, their responsibilities, leadership, and coordination with other applicable teams during a recovery operation. Insert hierarchical diagram of recovery teams. Show team names and leaders; **do not** include actual names of personnel. Names of personnel can change and for ease of document changes, will only be identified in Attachment 1.

Describe each team separately, highlighting overall recovery goals and specific responsibilities. Do not detail the procedures that will be used to execute these responsibilities, as these procedures will be itemized in the appropriate phase sections.

Example:Management Teams:

ISO
 Information System Security Official (ISSO)
 Chief Information Officer (CIO)
 Key Contingency Personnel
 Center Information Technology Security Manager (ITSM)

Functional Teams:

Data Center Server Support
 Application Support Team
 Damage Assessment Team
 User Support

Other teams include:

Contingency Plan Development Teams
Procurement Team
Recovery Team
Contingency Coordination Team
Disaster/Emergency Response Team
Acceptance Team

2.3 Information System Categorization

Security Objective	Ranking (Low-Mod-High)
<i>Confidentiality</i>	
<i>Integrity</i>	
<i>Availability</i>	
Security Category (SC) =	Select either Low, Moderate, or High according to the highest sensitivity ranking above

EXAMPLE	
Security Objective	Ranking (Low-Mod-High)
<i>Confidentiality</i>	Low
<i>Integrity</i>	Moderate
<i>Availability</i>	Moderate

<i>Security Category (SC) =</i>	Moderate
---------------------------------	----------

2.4 Mission Criticality

Discussion:

A system's mission criticality must be documented here. A Mission Essential Infrastructure (MEI) is a key resource/asset that the Agency depends upon to perform and maintain its most essential missions and operations. These resources may include critical components and facilities associated with the Space Shuttle, expendable launch vehicles, associated upper stages, Spacelab, International Space Station, command communication and control capability, Government-owned flight or experimental flight vehicles and apparatus, and one-of-a-kind irreplaceable facilities.

2.5 System Description and Architecture

Discussion:

Provide a general description of system architecture and functionality. Indicate the operating environment physical location general location of users and partnerships with external organizations/systems. Include information regarding any other technical considerations that are important for recovery purposes such as backup procedures. Provide a diagram of the architecture. Ensure to include identified known issues regarding the system.

[Insert Diagram Here]

2.6 System Interconnection/Information Sharing

Discussion:

System interconnection is the direct connection of systems for the purpose of sharing information resources. System interconnection, if not appropriately protected, may result in a compromise of all connected systems and the data they store, process, or transmit. It is important that system operators, information owners, and management obtain as much information as possible about the vulnerabilities associated with system interconnection and information sharing and the increased controls required to mitigate those vulnerabilities.

OMB Circular A-130 requires that written management authorization (often in the form of a Memorandum of Understanding or Agreement,) be obtained prior to connecting with other systems and/or sharing sensitive data/information. The written authorization shall detail the

rules of behavior and controls that must be maintained by the interconnecting systems. System owners are expected to document all interconnections, data dependencies and interdependencies in all system documentation. A description of the rules for interconnecting systems and for protecting shared data must be included with this plan.

In this section, provide the following information concerning the authorization for the connection to other systems (including the internet) or the sharing of information. List of interconnected systems and data dependencies and interdependencies:

- System Security Plan number (if NASA system)
- Name of system(s)
- Organization owning the other system(s)
- Type of interconnection (TCP/IP, Dial, SNA, SFTP, etc.)
- Name and title of authorizing management official(s)
- Date of authorization
- System of Record, if applicable (Privacy Act data)
- Security Categorization level

3. Notification and Activation Phase

This section addresses the initial actions taken to detect and assess damage inflicted by a disruption to *[System Name]*. Based on the assessment of the event, the plan may be activated by the ISO.

In an emergency / disaster, the *[Organization Name]*'s top priority is to preserve the health and safety of its staff before proceeding to the Notification and Activation procedures.

The *[System Name]* Contingency Plan Coordinator will be responsible for initiating notifications using the Emergency Team List that is in Attachment 1. When making notifications, begin at the top of the contact list and proceed downward until positive contact is made. The *[System Name]*'s Contingency Plan Coordinator is responsible for updating the emergency notification contact periodically or as needed as personnel assignments change.

Discussion:

The notification strategy should define procedures to be followed in the event that specific personnel cannot be contacted. Notification procedures should be documented clearly in the contingency plan. A common notification method is a *call tree*. This technique involves assigning notification duties to specific individuals, who in turn are responsible for notifying other recovery personnel. The call tree should account for primary and alternate contact methods and should discuss procedures to be followed if an individual cannot be contacted.

3.1 Damage Assessment Procedures

The Contingency Plan Coordinator, following an emergency event based on the damage assessment, will ensure implementation of this plan if needed. It is imperative that the nature of the emergency and the extent of the damage be assessed as quickly as conditions allow. Details of damage assessment procedures are located in Attachment 2.

Discussion:

CPC is expected to conduct a damage assessment of IT components (application) and supporting components in accordance with business and operational requirements. This analysis should be detailed enough to provide adequate information for plan activation.

3.2 The Contingency Plan Activation

Discussion:

This section will document the criteria used for activating the Contingency Plan. The Contingency plan should be activated only when the damage assessment indicates that one or more of the activation criteria for that system are met. If an activation criterion is met, the CPC

or CIO (as appropriate) should activate the plan. Activation criteria for events are unique for each organization and should be stated in the contingency planning policy statement. Criteria may be based on:

- Safety of personnel and/or extent of damage to the facility
- Extent of damage to system (e.g. physical, operational, or cost)
- Criticality of the system to the organization's mission (e.g., critical infrastructure protection asset)
- Anticipated duration of disruption

ISOs are required to document criteria for activation. However, due to the cost of activating a contingency plan, ISOs should consider criteria for non-activation.

[System Name] Contingency Plan Activation Criteria

- The damage assessment reveals critical components supporting the system will be unavailable for more than 24 hours.
- ISOs should document other criteria as they apply to the system

[System Name] Plan Activation Exclusions

- Activation of COOP/DRP
- Agency wide outage beyond system control
- Planned outages or service disruptions
- ISOs should document other exclusions as they apply to the system.

Notification and Activation Roles and Responsibilities

- When the plan is activated, the CPC is to notify all Team Leaders and inform them of the details of the event and if relocation is required.
- Upon notification from the CPC, Team Leaders are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary.
- The CPC is to notify the *off-site storage facility* that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the *alternate site*.
- The CPC is to notify the Alternate site, if applicable, that a contingency event has been declared and to prepare the facility for the *Organization's* arrival.
- The CPC is to notify remaining personnel (via notification procedures) on the general status of the incident.

3.3 Alternate Location Procedures

The CPC will be responsible for contacting appropriate personnel and all other appropriate agencies immediately of the agency's alternate location, operational and communications status, and anticipated duration of relocation, if known.

Discussion:

Enter appropriate information in the box below, if applicable.

Name of Alternate Facility	Address

4. Recovery Operations Phase

Discussion:

This section focuses on procedures for recovering the application at the alternate site, whereas other efforts are directed to repair damage to the original system and capabilities.

When a disruption occurs, despite the preventive measures implemented, a recovery strategy must be in place to recover and restore data and system operations within the recovery time objective period. The recovery strategy is designed from a combination of methods, which together address the full spectrum of information system risks.

NOTE: The most cost-effective option, based on potential impact, are selected and integrated into the information system architecture and operating procedures.

The following procedures are for recovering the *[System Name]* at the alternate data center. Procedures are outlined per team required. Each procedure should be executed in the sequence it is presented to maintain efficient operations.

4.1 Recovery Procedures and Objectives

Discussion:

State recovery procedures and objectives as determined by the Business Impact Analysis (BIA). For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures. Include the following at a minimum:

What personnel have the access privileges to the offsite storage facility?

Who is the offsite Point of Contact (POC)?

What type of restoration can be performed from the alternate site - full, partial?

As a part of restoration/recovery, do transaction logs automatically update master files?

How do non-captured transactions get re-entered?

Example:

Depending on the nature of the system outage, a combination of recovery procedures should be implemented by the Recovery Team. Recovery procedures listed in this section provide the CPC with high-level guidance regarding the types of activities to be performed during contingency operations. Additionally, Attachment 3 contains an action item checklist to assist the CPC track these operations.

While monitoring recovery operations, the CPC should notify the ISO to escalate the situation to higher management if it is likely that the system will not be recovered within 48 hours.

If the building that houses the failing [System Name] component(s) is damaged or has been evacuated, the CPC contacts the datacenter management for assistance in obtaining an estimated time that recovery personnel may safely reenter the building to begin supporting [System Name] contingency plan operations.

The CPC should coordinate with the datacenter management to obtain information on the physical environment of the computer room that houses the application and get an estimated time that the building will be cleared for reentry by Agency personnel.

The CPC should provide periodic updates regarding the reopening of the datacenter and the restoration of facilities services.

The Recovery Teams so designated in the plan are responsible for the recovery of the IT Infrastructure (e.g., LAN/wide area network (WAN), server, database) and the reinstallation of the application.

Support personnel should refer to their standard operating procedures for recovery of all IT components. This includes reinstalling all hardware and software (operating system, etc.) that serves as the platform of the application. System administrator and application recovery personnel should reference the application's maintenance manual for step-by-step procedures and supporting documentation. Support personnel should also contact all vendors to provide additional support as needed.

The Application Recovery Team works in conjunction with the network and system administrator Recovery Team personnel to ensure a seamless restoration of the application's software and data.

5. Reconstitution Phase

This section discusses activities necessary for restoring *[System Name]* operations at the *[Organization Name]*'s original or new site. When the computer center at the original or new site has been restored, *[System Name]* operations at the alternate site must be transitioned back.

Once the original site is restored or new site is operational to the level that it can support the IT system processes, the system may be transitioned back to the respective data center. Until the primary location is restored and operational and the system has been tested at the original or new site and deemed operational, the contingency data center should be maintained and utilized. The goal is to provide a seamless transition of operations from the contingency (alternate) site to the original or new data center.

5.1 Concurrent Processing

Discussion:

Outline in this section, the procedures (per necessary team to be aligned with teams identified in section 2.2.1), to operate the system back at the original or at the new site. These procedures should include testing the original or new system until it is functioning properly and the contingency system is shut down gracefully.

{team name}

- Team Resumption Procedures

{team name}

- Team Resumption Procedures

5.2 Plan Deactivation

Discussion:

Procedures must be outlined, per team, to clean the alternate site of any equipment or other materials belonging to the organization, with a focus on handling sensitive information. Materials, equipment, and backup media must be properly packaged, labeled, and shipped to the appropriate location(s) in accordance with the NASA security policy. Team members must be instructed to return to the original or new site.

6. Training, Testing and Exercises

To ensure an effective and viable [System Name] contingency planning capability, periodic training, testing, and exercises (TT&E) should be conducted on the [System Name] contingency plan. This process will range from exercising parts of the plan (e.g., Notification phase) to full-scale tests of the entire [System Name] recovery and resumption process. This section presents procedures and standards for developing a TT&E program. It also discusses methods for maintaining, updating, and distributing the contingency plan to all responsible personnel to ensure an active state of readiness.

A successful contingency plan depends on the ability of Agency personnel to perform their responsibilities efficiently and correctly. Training provides an effective means of enhancing individuals' familiarity with the contingency plan and increases their ability to implement the plan properly. NASA personnel must receive training on the contingency plan and participate in hands-on contingency planning exercises. New personnel with contingency plan responsibilities will receive a copy of the current contingency plan and an orientation on its use. Personnel will periodically review the contingency plan to refresh their knowledge of the procedures. Thus, when responding to a disaster or contingency, they can respond accordingly.

6.1 Contingency Plan Testing and Exercise

Since the contingency plan is a living document, regular testing and evaluation are an essential part of plan maintenance. Testing familiarizes personnel with the contingency planning process by simulating notification/activation, recovery, and resumption processes, and identifies key areas in which Recovery Team members may require additional training or orientation concerning the [System Name] contingency plan. Contingency plan testing should be coordinated by the CPCr and the Program Office Information System Security Officer (ISSO) to ensure that all major elements and components of [System Name] are tested. A testing schedule has been developed that includes the time frames and participants for the main testing steps: developing the test plan, executing the test plan, and documenting the test plan results and recorded in Attachment 4 and 5. All testing must be performed at least annually to ensure that the contingency plan could be relied on in the event of a system failure.

6.2 Documenting Test Plan Results

The test plans and the results of the tests is documented and maintained as part of the overall contingency plan documentation. The latest test results are documented in Attachment 5. Documentation helps in evaluating liabilities and identifying achievements. Once the test plans and their results have been documented, the CPC should forward the documentation to the ISSO and ISO for review. The ISSO and ISO must sign off on the documents to indicate that the plan was successfully tested. This documentation will serve as a record of "observations" and will assist in determining which procedures worked well and which need to be modified.

6.3 Plan Maintenance

As a living document, the contingency plan must be maintained and updated over time. The [System Name] ISO is responsible for maintaining, testing, and updating the plan. However, the ISO may delegate all or parts of this responsibility to the CPC, or others, as appropriate. The ISO should coordinate with key individuals in planning TT&E schedules and objectives, analyzing TT&E documentation (e.g., observations and results), and monitoring major changes to [System Name]. To ensure that the plan maintains a current state of readiness, it is important that the ISO keep the following maintenance schedule:

- Review and update the plan annually or more frequently based on significant changes to the [System Name] application architecture
- Review and update the contact sheets and vendor information semi-annually or more frequently based on significant changes to Agency [System Name] personnel, vendors, and supporting contractors
Update the plan when test results indicate procedural changes.

When a small change to the plan is necessary, it may be inserted into the existing plan and documented by the [System Name] CPC in the Record of Changes table rather than rewriting and updating the entire plan. All changes must be tracked in the record of changes and distributed to all personnel with plan responsibilities.

Table 1: [System Name] Plan Maintenance

Activity	Tasks	Frequency
Plan maintenance	<ul style="list-style-type: none"> - Review entire plan for accuracy of operational procedures, technical components, configurations, controls, and organizational structure - Incorporate 'lessons learned' and change in policy and philosophy - Manage distribution of plan updates 	<ul style="list-style-type: none"> - Annual (at least) general update - Semiannual updates of personnel contact information - With significant changes to components, configurations, organization structure, or controls - Following tests and exercises
Train new members	<ul style="list-style-type: none"> - Provide orientation and training class - Schedule participation in all training and exercise events 	<ul style="list-style-type: none"> - Within 3 months of hiring personnel with contingency plan responsibilities
Orient new policy officials and senior management	<ul style="list-style-type: none"> - Brief key personnel on [System Name] contingency plan - Brief all key personnel on their responsibilities under the contingency plan 	<ul style="list-style-type: none"> - Annually - When redistributing the plan - When adding new key personnel
Review and update Notification, Activation,	<ul style="list-style-type: none"> - Review and update Notification procedures - Review and update 	<ul style="list-style-type: none"> - Annually, or as needed

Activity	Tasks	Frequency
Recovery and Resumption phases	Activation procedures - Review and update Recovery procedures - Review and update Resumption procedures	
Review and update IT CP roles and responsibilities	- Update key personnel POC information	- Semiannually, or as needed
Plan and conduct exercises	- Develop scenario, schedule, objectives, and success criteria - Conduct walkthrough exercises - Conduct joint exercises with Agency personnel and supporting contractors - Document and review lessons learned	- Annually (at least), or as needed

The ISO is responsible for distributing the contingency plan. Two copies of the contingency plan should be distributed to those responsible for coordinating the plan and those who participate in recovery and resumption operations. Each person is required to maintain one copy at the plan holder's office, and the other copy should be kept at the plan holder's home for after-hours emergency situations. The original document is to be stored at a secure location that is easily accessible by both the ISO and the CPC. If there is a change to the plan, the entire obsolete contingency plan or obsolete page(s) must be retrieved or confirmed to have been destroyed by all personnel before the new or updated plan or pages are distributed. This practice will ensure that all personnel maintain the most current contingency plan and that contingency operations can be completed efficiently. All key personnel are required to fully examine the contingency plan to better understand their roles and responsibilities.

Attachment 1: Emergency / Disaster Team Formulation

Fill in the following tables as appropriate. Develop a flow diagram to show how these teams will interact.

Contingency Plan Development Teams

1. Contingency Plan Work Group

The Contingency Plan Work Group supports the Contingency Plan Coordinator in the development of strategies to restore critical business function in the event of an emergency or disaster. The work group completes all preliminary activities, including selecting team members and reaching agreements on offsite storage and alternate facilities.

Title	Name	Work Phone	Home Phone	Alt. Phone
Contingency Plan Coordinator				
Alternate Cont. Plan Coordinator				
Team Member				
Team Member				

2. Procurement Team

The Procurement Team acquires any required hardware/software and related documentation and/or other items that must be placed at the alternate facility.

Title	Name	Work Phone	Home Phone	Alt. Phone
Team Lead				
Alternate				

Team Lead				
Team Member				
Team Member				

Recovery Teams

1. Restoration Management Team

The Restoration Management Team is responsible for determining the best course of action for restoring critical business functions in the event of an emergency or disaster.

Title	Name	Work Phone	Home Phone	Alt. Phone
Restoration Manager				
Alternate Restoration Manager				
Team Member				
Team Member				

2. Contingency Coordination Team

The Contingency Coordinator is responsible for informing Agency management about the status of efforts to restore critical business functions in the event of an emergency or disaster and ensures the coordination of restoration activities at the alternate facility. The Contingency Coordination Team conveys management instructions and disseminates status information to leaders of other teams.

Title	Name	Work Phone	Home Phone	Alt. Phone
Contingency				

Coordinator				
Alternate Contingency Manager				
Team Member				
Team Member				

3. Disaster/Emergency Response Team

The Disaster / Emergency Response Team assesses the functionality of systems, conducts and initial damage assessment, and provide ongoing status reports in the event of an emergency or disaster. After the Disaster / Emergency Response Team assess' an incident, members may disperse to lead or participate in other teams.

Title	Name	Work Phone	Home Phone	Alt. Phone
Team Lead				
Alternate Team Lead				
Infrastructure Representative				
Network Operations Representative				
Server Administration Representative				

4. Recovery/Restoration Team

The Recovery/Restoration Team has overall responsibility for restoring a system, either partially or fully, as instructed by the Restoration Management Team.

Title	Name	Work Phone	Home Phone	Alt. Phone
Recovery/Restoration Coordination				
Alternate Recovery/Restoration Coordination				
Team Member				
Team Member				
Team Member				

5. Acceptance Team

The Acceptance Team is responsible for conducting functional testing on and for accepting or rejecting a restored system after an emergency or disaster. A case for accepting a system with limited capabilities must be justified to Agency management, which is responsible for declaring the system operational.

Title	Name	Work Phone	Home Phone	Alt. Phone
Acceptance Coordinator				
Alternate Acceptance Coordination				
Team Member				
Team Member				
Team Member				

6. Additional Notification Contact List

PRIMARY					
NAME	WORK PHONE	HOME PHONE	CELL / PAGER	TIME CALLED	CONTACTED YES/NO
ALTERNATE					
NAME	WORK PHONE	HOME PHONE	CELL / PAGER	TIME CALLED	CONTACTED YES/NO

7. Vendor Contact List

Hardware/ Software	Asset	Vendor	Point of Contact	Phone
<i>Hardware</i>	<i>Web Server</i>	<i>ACME</i>	<i>John Doe</i>	<i>555-1212</i>

Attachment 2: Damage Assessment Checklist

The following report is to be used by the Recovery Teams in developing an assessment of the system failure.

DAMAGE ASSESSMENT REPORT	
Name:	
Event Information	
Date:	Time of Incident:
Location:	Type of Event:
Impact to System:	Facility Damage:
Personnel Injuries:	
System Information	
Point of Contact (POC):	Estimated Length of Disruption:
Impact on Components:	
Component Resources Affected:	
Type of Damage to Resource:	
Estimated Equipment Needs:	
Recovery Information	
Suggested Recovery Strategy:	

Activation of Contingency Plan Recommended: (Y) (N)

CPC Signature: Date/Time

ISO Signature: Date/Time

AO Signature: Date/Time

Attachment 3: Contingency Log and Action Item checklist

Example Template

Task	Completed	Time
SYSTEM DISRUPTION—INITIAL NOTIFICATION	(✓)	
1. The Contingency Plan Coordinator (CPC) contacts the XXXX Group and instructs them to perform a damage assessment.		
DAMAGE ASSESSMENT PROCEDURES	(✓)	
2. Complete Damage Assessment Report (Attachment 2).		
a. Check the cause of the system disruption, including type, scope, location, and time of incident.		
b. Check whether the outage is localized (this system only) or widespread.		
c. Check the location of failing components and those users without service.		
d. Check the impact of the disruption or components damaged.		
e. Check the functional status of all system components (e.g., fully functional, partially functional, nonfunctional).		
f. Check the potential for additional disruption or system damage.		
g. Check the identification of a single point of failure (if possible).		
h. Check items to be replaced (e.g., hardware, software, firmware, supporting materials).		
i. Check anticipated downtime of the application (e.g., longer than 2 days).		
j. Classify disruption as Minor System Failure or Major System Failure.		
MINOR SYSTEM FAILURE	Completed	
Recovery and Resumption Procedures	(✓)	
3. The Recovery Teams contact the CPC to provide an estimated recovery time and begin repair of the components (i.e., the databases, servers, infrastructure or the application software).		
4. The CPC notifies all [SYSTEM NAME] users that the Minor System Failure is being recovered and will be functioning under normal conditions within the estimated recovery period. Users are also notified via the Hot News bulletin.		
5. Minor System Failure is recovered and incident is closed.		
MAJOR SYSTEM FAILURE	Completed	

Task	Completed	Time
Notification/Activation Procedures	(✓)	
6. The CPC reviews the damage assessment report and contacts the ISO to activate the contingency plan formally.		
7. The CPC contacts all [SYSTEM NAME] user groups, alerting them of a major system outage and expected recovery time. Additionally, the CPC contacts the IT Management, the [SYSTEM NAME] Help Desk, and Program Office, which will notify additional user groups.		
8. The CPC contacts all required Recovery Team personnel to initiate system or application recovery.		
Recovery Procedures – Building and Facilities Services	(✓)	
9. The CPC coordinates with the Data Center manager to obtain an estimated downtime – once the building has been cleared for reentry.		
10. The CPC provides the ISO with periodic updates on reopening of the Data Center and restoring facilities services.		
Recovery Procedures – IT Infrastructure	(✓)	
11. The CPC will contact all required Recovery Team personnel to begin contingency operations. <ul style="list-style-type: none"> a. The Recovery Teams are responsible for recovering (servers, database, etc.) and reinstalling the application code. b. Support personnel should refer to their standard operating procedures for recovery of all IT components; this includes reinstalling all hardware and software (i.e., operating system, etc.) that serves as the platform of the application. Personnel should reference the application’s maintenance manual for step-by-step procedures and supporting documentation. c. Support personnel also should contact all vendors to provide additional support as needed. 		
12. The Recovery Team is also primarily responsible for obtaining and restoring data from backup facilities to assist in restoring all components.		
13. The CPC contacts the ISO when the IT Infrastructure has been recovered, and contingency operations move into the resumption phase if the application is operating under normal conditions.		
Recovery Procedures – Application Software	(✓)	
14. The CPC notifies the Application Recovery Team to begin recovery operations of the application software.		

Task	Completed	Time
15. The Application Recovery Team works in conjunction with the Recovery Team personnel to ensure a seamless restoration of the application's software and data.		
16. The CPC contacts the ISO to provide periodic updates on recovery operations as they are received from the Application Recovery Team.		
17. The CPC contacts the ISO when the application software has been recovered, and contingency operations move into the resumption phase if the application is operating under normal conditions.		
RESUMPTION PROCEDURES	(✓)	
<p>18. Upon recovery of the affected [SYSTEM NAME] components, testing of the components and application should be performed to ensure proper functionality. Recovery Team personnel should test all recovered components and the application using a logical sequence to ensure complete functionality has been restored.</p> <ul style="list-style-type: none"> a. An Application Test Plan is provided in the Appendices for Application Recovery Team to use for testing purposes – this test plan is designed to test the application's functionality from the user's perspective. b. Screen captures depicting the results of the Application Test, should be saved and forwarded to the CPC as a record that testing was completed and that the application is functioning under normal conditions. These must not contain personal identifiers. c. If the reinstalled application fails any testing activity, the Application Recovery Team should coordinate with personnel to properly identify and correct the application failure. 		
19. Upon completion of all testing activities, the CPC notifies the ISO that the application has been tested and is functioning properly.		
20. Recovery Teams return all materials, plans, and equipment used during recovery and testing back to storage.		
21. All sensitive material is destroyed or properly returned to safe storage.		
22. Recovery Team personnel assisting other offices conclude their activities and report to their primary sites.		
RESUMPTION PROCEDURES	(✓)	
23. The CPC notifies the user groups on resuming normal business operations.		
24. The CPC develops an after-action report and files it with the ISO.		

Attachment 4: Contingency Plan Test Strategy

Discussion: The purpose of this section is to document the procedures that will be followed to test this document and its functionality. The Contingency plan testing verifies the effectiveness of a system's controls against anticipated outages for unanticipated interruptions. This identifies the approach used for testing, the testing team, and the results of the testing activity. The testing requirement is stated in NIST SP 800-34, NPR 2810.1 (NITR 2810-15) and the NASA SOP-0040, Contingency Planning Guidance. Testing is required annually and will increase in intensity over a three-year time period. Variance depends on the systems' category in accordance with FIPS 199. After the three (3) years' tests have been completed, the schedule will repeat itself. Below provides the system category and the year required testing type. Identify which System Category is relational to the system and which year and test type is being/ has been conducted.

A recommended schedule for testing is as follows:

The tests will increase in intensity over a three-year time period and vary based on the FIPS 199 system category. After the Year 3 tests have been completed, the schedule should repeat, starting with Year 1.

System Category	Year 1 – Test Type	Year 2 – Test Type	Year 3 – Test Type
Low	Classroom Exercises/Tabletop Written Test	Classroom Exercises/Tabletop Written Test	Classroom Exercises/Tabletop Written Test Integrated Test
Moderate	Classroom Exercises/Tabletop Test	Classroom Exercises/Tabletop Test with Scenarios	Functional Exercises/Simulation Exercise Integrated Test
High	Functional Exercises/Simulation Exercise	Functional Exercises/Simulation Exercise	Functional Exercises/Alternate Site Test Integrated Test

The Contingency Plan should be maintained routinely and exercised/tested at least annually. Contingency procedures must be tested periodically to ensure the effectiveness of the plan. The scope, objective, and measurement criteria of each exercise will be determined and coordinated by the CPC on a "per event" basis. The purpose of exercising and testing the plan is to continually refine resumption and recovery procedures to reduce the potential for failure.

EXAMPLE

[System Name] Contingency Plan 3 year Test Schedule

Schedule Test Date Year 1: 01/2008

THE PROGRAM OFFICE WOULD SCHEDULE ABC INFORMATION SYSTEM FOR A TABLE TOP/CHECKLIST TEST 2ND QUARTER FY08.

Objective

To determine the feasibility of the contingency plan recovery strategy and determine whether the recovery solutions are possible in a real contingency scenario, whether any flaws need to be eliminated and contingency teams and supporting parties are able to achieve its objective indicated in the plan.

Testing Type

Table Top/Checklist

Scope of Testing

The ability to process ABC System mission within the maximum allowable outage time.

Software: Cold Fusion Application Code

- Client Executable Software

- Oracle Database Schema

- Oracle Database Data

Scenario

ABC Information System has suddenly failed. System Technical Point of Contact have placed a call to the help desk and the technicians have determined that the problem is not workstation or communication related. The technicians have found your database code has been corrupted and the application is not functioning.

Required Participants

ISO

Technical Point of Contact

Support Staff

Database Administrator

Program Administrator

Program Developer

Schedule Test Date Year 2: MM/YYYY

Objective

Testing Type

- Table Top/Checklist
- Structure Walkthrough

Scope of Testing

Scenario

Required Participants

Schedule Test Date Year 3: MM/YYYY

Objective

Testing Type

- Table Top/Checklist
- Structure Walkthrough

Scope of Testing

Scenario

Required Participants

Attachment 5: Contingency Plan Test Results

The following provides an Contingency Plan Test Results Example. Revise this plan to incorporate the appropriate test results of the system.



National Aerospace and Space Administration
WASHINGTON, DC

Date (ex. June 1, 2008)

**OFFICE OF THE CHIEF INFORMATION OFFICER
SENIOR AGENCY INFORMATION SECURITY OFFICIAL**

Subject: Annual [System Name] Contingency Plan Testing

PURPOSE

Contingency plan testing is essential to ensure that information systems are able to continue processing during a planned or unforeseen outage. Testing is used to determine the accuracy of recovery procedures and identify deficiencies in maintaining processing requirements.

FISMA section 3554(b) (8) requires that NASA's information security program include plans and procedures to ensure continuity of operations for information systems that support the Agency's operations and their assets.

A [**type of contingency test**] was conducted on [month/date/year](#). The observations were documented for system compliance in accordance with the Agency's IT Security Policy and Federal laws to ensure the ability to restore essential IT functions in the event of a contingent incident.

TESTING APPROACH

The basic approach to contingency plan testing [**type of contingency test**] is to determine the accuracy of recovery procedures and identify deficiencies in maintaining processing requirements. Information Technology contingency plan requirements consist of those items identified in NIST SP 800-34 in addition to specific Agency requirements.

The methods for testing and evaluating include:

- **Inspection** – examination or review system contingency planning documents, application restoration and installation procedures and assets, such as review of a configuration file or software version number.
- **Test** – the evaluation and analysis through systematic hands-on measurement under appropriate conditions and scenarios.

-
- **Demonstration** – the evaluation of operation restoration will not be required during this level of testing.

Testing techniques will consider threat and vulnerability information from both government and industry sources to evaluate a comprehensive range of possible outage scenarios. Emphasis is placed on the existence of application controls as well as evidence of contingency planning as an integral part of the business environment. Problems that are identified during the testing activity can be immediately corrected or may be identified as items of concern, which are discussed in detail in the mitigation plan or task list.

TEST SCENARIO:

A worst-case scenario was used to test the ability of the system to be recovered and restored. This scenario is based on assumptions that the requirements for the system is not altered by the emergency; that funding and personnel are available; that interconnectivity with the Local Area Network (LAN) is available; that the alternate processing site is available; and that all supporting plans are viable. In the event of an operational incident¹ the incident may be used as an actual test of the program offices' contingency plan.

PRIMARY OBJECTIVES:

- **Objective 1:** To determine the familiarity of personnel with the plan and determine whether contingency plan duties and responsibilities are clearly defined including line of succession for senior management authority and plan activation authorization.
- **Objective 2:** To determine the feasibility of the contingency plan recovery strategy and determine whether the recovery solutions are possible in a real contingency scenario, whether any flaws need to be eliminated and contingency teams and supporting parties are able to achieve its objective indicated in the plan.

SECONDARY OBJECTIVES:

- **Objective 1:** To determine the degree to which the contingency plan has been documented, whether the state of the plan is current and has been properly maintained and upgraded to meet the current recovery needs of the organization, and whether senior management has identified and documented key IT processes and resources, maximum allowable outages and organization recovery priorities.
- **Objective 2:** To determine the availability of recovery resources, whether the recovery alternatives at an alternate site are adequate to restore computer processing, and to evaluate that the vendor solution are workable in accordance with the organization's needs.

TEST CHRONOLOGY:

- **Times/Dates of Pre-Test Activities:** Test Coordination was affected on or about [Month/date/year](#) as part of an overall contingency planning initiative. **This section**

should also note any communication or assistance provided with the contingency plan document, to the program office.

- **Times/Dates of Major Test Activities:** The [type of contingency test] was conducted on Month/date/year at time a.m. or p.m.
- **Times/Dates of Post-Test Activities:** The Test Results Report was prepared on Month/date/year.

PARTICIPANTS:

- *Name Program Office, Position/Company, Phone*
- *Kelvin Taylor, Office of Chief Information Officer IT Security, Contingency Plan Coordinator, 202 708 4505 ext 2809*
- *Harry Bordeaux, CIO: Indoor Basketball, (202) 555-1212*
- *Earnest Borgnine , ISO, McHale's Division, (202) 708-2121 Ext. 7609*
- *Dolly Pardoner, ISSO, Nashville Convention Center 202. 555-1212*

SCOPE OF TEST:

- **Processes:** Define the business/purpose of the system. (e.g. *Air Crew Scheduling.*)
- **Software:** *Windows 2000 and Oracle 10*
- **Program Office(s)/Supporting Organization(s):** *Housing; ABC Corp.*
- **Location(s):** *NASA Headquarters, 300 E St SW, Washington D.C. 20410*

OBSERVATIONS (document all results from testing):

- **Observation 1:** The contingency plan does not address functional team roles (i.e., CPC, Application Administrator, and Team Managers), responsibilities of personnel involved in the application recovery of [system name] or contain a list of point of contact for team members. System support personnel do not have documented processes or procedures in place once a system disruption has been detected.
- **Observation 2:**
- **Observation 3:**

RECOMMENDATIONS (document recommended actions to be taken to remedy observations):

- **Recommendation 1:** The Contingency Plan should be updated to reflect roles and responsibilities of contingency team members. Once completed, the ISO should ensure that each individual involved in the recovery/restoration of the system review the plan and conduct joint training on the plan based on documented test schedule.
- **Recommendation 2:**
- **Recommendation 3:**

APPROVAL:

I certify that the facts, findings, and recommendations of the Test Results Report accurately record the results of the Structured Walk-Through Test conducted on the [ABC system](#) conducted on [Month/date/year](#).

Contingency Plan Coordinator: _____

Signature: _____

Date: _____

Based on my review of [ABC System](#) Contingency Testing Results Report, I concur with the findings and will take appropriate action to maintain restoration documentation and strategies consistent with documented recovery requirements.

Program Office ISSO: _____

Signature: _____

Date: _____

Information System Owner: _____

Signature: _____

Date: _____

Appendix D: Example NASA Tabletop Exercise Plan and Written Test

EXAMPLE NASA TABLETOP EXERCISE PLAN AND WRITTEN TEST



<System Name>

<SSN Number>

<Organization>

Contingency Plan Tabletop Written Test

Example NASA Tabletop Exercise Plan and Written Test

The sample written test can be used as the primary test for low-impact systems or as a first step to test moderate- and high-impact systems. This test can be modified to address specific Program Office areas of concern.

1. Introduction

After system contingency plans are documented, it is critical that these plans be tested to ensure that the recovery process is not only well documented, but also understood by the staff responsible for the recovery. Several types of tests can be executed to verify if a contingency plan is viable and effective, as well as if personnel (i.e., Agency employees and third-party service providers) are well trained in all aspects of the recovery and restoration processes documented in the Contingency Plan. Agency testing strategy calls for three testing levels—tabletop, simulation exercises, and alternate site. Each testing level has its own objectives and each level has increased degrees of complexity as listed below:

- **Tabletop Test**—most informal contingency testing procedure. It is designed to test the knowledge and awareness of the teams and to ensure that participants are aware of their roles and participation in the processes to recover data and systems.
- **Simulation Exercise**—more advanced test. A simulation exercise uses the existing Contingency Plan and measures its effectiveness against a fictional series of calamitous events. All responsible staff should be present at the simulation, as well as a representative from each business unit.
- **Alternate Site Test**—transfers operations to the alternate restoration facility. This test is used to ensure that the alternate site operates as planned during the recovery process and after the system has been recovered. Third-party vendors may be included in this test.

This document focuses on table top test strategy.

2. Table Top Test Objectives

There are three objectives for table top testing:

- Verify that all Recovery/Restoration Team members understand their role in the recovery of a system. In order to meet this objective, all team members must do the following:
 - Have a copy of the latest Contingency Plan
 - Become familiar with the Contingency Plan
 - Understand the plan, anticipate the sequence of events leading to a system recovery, and know their precise individual roles and responsibilities to support an effective recovery
 - Understand how to interact with other teams that are also assisting in the recovery effort
 - Know their own team members, as well as other team leads
 - Keep in their possession, both onsite and offsite, the pertinent information needed to perform their recovery duties
 - Have the media, other materials, and tools needed to ensure an effective recovery
 - Resolve all questions and ambiguities during the table top test

-
- Improve the Contingency Plan by modifying the plan based on discussions, observations, and findings identified during the table top test.
 - Provide Agency's management and team leads with a test summary. This summary, prepared by the test moderator, should outline successes and areas for improvement.

3. Test Assumptions

The following assumptions are made, which were specifically designed for the table top test, to ensure that the test is effective:

- The test will take place after individual contingency plans have been completed.
- The test will take place even if some team members cannot attend, which simulates actual situations that may occur during an emergency.
- The organization has officially assigned well-suited individuals to the various Recovery/Restoration Teams. The position description for individuals participating in the contingency operations was updated to reflect their assigned responsibilities.
- All team members have a copy of the Contingency Plan and its appendices, have read the plan, and have an understanding of their team roles, as well as the roles of teams with whom they interact.
- All team members will bring their personal copy of the plan to the test and refer to it when needed.
- All participants are cleared to enter the facility and the conference room for testing.

4. Test Scope

The scope of the table top test consists of written and verbal acknowledgement by team members of their recovery and restoration responsibilities, as well as a demonstration of their knowledge of the recovery process and their specific duties within this process. The test is limited to questions (presented by the test moderator), answers (by team members), and discussions. Team members are encouraged to ask the moderator for clarifications when ambiguous points and issues are discussed.

The scope does not include any hands-on use of equipment that is used during an actual recovery (e.g., phone system, tape backup unit, server, and router). The scope does not include a walk-through of the alternate relocation site.

The test is limited to the system covered by the Contingency Plan. A disaster may affect infrastructure components for which members have no restoration responsibilities. In future tests, when an infrastructure component (e.g., air conditioning [AC], electricity, or network) failure brings down the system under consideration, the test should include demonstrating an understanding of how the Recovery/Restoration Team will interact with recovery personnel involved in the facility restoration process.

5. Roles and Responsibilities

The Contingency Plan identifies the teams listed below as instrumental in the recovery from an emergency. Specific contingency plans may include some of these teams, all of these teams or additional teams the contingency planning groups may consider necessary. The table top test includes only those teams listed in the system's Contingency Plan.

Contingency Plan Work Group

The Contingency Plan Work Group completes all preliminary activities, including agreements for offsite storage and space at the alternate operating facilities. The Work Group supports the Contingency Coordinator in developing strategies to keep the organization's critical Information Technology (IT) functions operational.

Restoration Management Team

The Restoration Management Team has the overall responsibility for handling the disaster (after a disaster has been declared) and deciding the best course of action needed to restore operations both onsite and offsite.

Emergency Response Team

The Emergency Response Team is responsible for assessing the overall adverse event's impact on safety, health, and operations, as well as predicting how long it will take (if possible) before full recovery can be achieved onsite. The team's *Damage Assessment Report* will be used by the Restoration Management Team to decide whether to relocate operations to the alternate site.

Contingency Coordination Team

The Contingency Coordinator is the focal point for conveying instructions from the Restoration Management Team to team leaders and for disseminating status information to all team leaders. The Coordinator is supported by an appropriate size team.

Recovery/Restoration Team

The Recovery/Restoration Team has the overall responsibility for restoring the system to its full/partial capabilities, whether onsite or offsite, as instructed by the Restoration Management Team.

Acceptance Team

The Acceptance Team has the overall responsibility for the functional testing of the restored system and then accepting or rejecting it. Acceptance of limited capabilities must be justified to the Restoration Management Team. The actual declaration that a system is fully or partially restored is made by the Restoration Management Team.

6. Success Criteria

The test will be considered a success if all its objectives, as listed in Section 2, were met and if the test moderator determines that all participants have sufficient knowledge of the plan, their roles and responsibilities, and the means needed to perform their recovery duties effectively. The test report, developed by the moderator after the test is completed, will identify the perceived level of success, as well as recommendations for improvements.

7. Test Logistics

There are few logistical test requirements because no actual or simulated hardware or software will be used during the table top test. Computer hardware, software, tools, supplies, meals, and beverages are not needed. Other test logistics include:

- Schedule—test is scheduled to last two hours. Exact dates and times will be coordinated with all participants by the contingency Coordinator

-
- Facility—team members must be present for this test—they cannot participate via a conference call.
 - Communications—projector is needed; however no computer equipment is needed—moderator will bring own laptop.

8. Technical and Business Impacts

Table top tests do not impact a system's operational status or the user community; however, there may be some impact on the support level for the system since many participants are responsible for the system's operation and support. It is the system owner's responsibility to verify that a sufficient level of user and technical support is maintained during the two hours allocated to take this test.

9. Test Activities

This section contains scenarios to be used during the table top test. The following three disaster scenarios may be presented to the participants. Questions asked will be answered relative to each scenario presented (see Appendix A). Often, the answers will be the same regardless of which scenario; however, some activities may be different depending on the scenario.

Scenario One: Local Failure

The AC system in the data center failed over the weekend causing computer equipment to overheat—the remote alarm system was accidentally turned off. As a result, two small computer system interface drives in the disk array used by the system have crashed rendering the system inoperable.

Scenario Two: Building Failure

A fire on the eighth floor caused a building evacuation. Neither the data center nor system users are located on the eighth floor; however, for safety reasons the fire marshal decided to disconnect power to the entire building until the fire is completely under control and a full damage assessment is available. There are no indications of how long this will take.

Scenario Three: Regional Failure

Terrorists attacked the local transportation system (e.g., subway) with what is suspected to be a chemical weapon. A train in the L'Enfant Plaza Metro station was attacked, causing a shutdown of the entire Metro system. The federal government declared a regional disaster and instructed all federal employees within a five-mile-radius from L'Enfant Plaza to evacuate and wait at their homes for further instructions. Electricity and data communications services were not disrupted and continue to operate normally. The local phone system (both landlines and cellular) is under heavy load and operates only marginally.

Note: The test may be stopped by the moderator if a determination is made that participants do not have sufficient knowledge or an understanding of the Contingency Plan.

Appendix A. Test Questions to NASA Tabletop Test Strategy

Appendix A consists of the list of questions asked to all team members, as well as specific teams, during the table top test. It includes questions for the following:

- All Team Members
- Restoration Management Team
- Emergency Response Team
- Contingency Coordination Team
- Recovery/Restoration Team
- Acceptance Team

A-1. Questions for All Team Members

1. Have you brought your copy of the plan?
2. Do you have a copy of the plan at home in case a disaster is declared after hours or a building emergency evacuation is ordered?
3. Have you read the plan?
4. What contingency planning training have you attended?
5. Do you have any major concerns about the effectiveness of the Contingency Plan for your system?
6. How would you be notified that a disaster has been declared?
7. Do you have instructions on what to do if the phone network is down and the building has been evacuated? Where will you work from if the building is evacuated for a prolonged period?
8. Can you name the team members that support contingency activities for your system?
9. Which procedures in the plan's appendices will your team use after a disaster has been declared?
10. Have you ever executed and tested these procedures to verify that they are effective?
11. Who provides instructions to your team? Who does the team report status and progress to?
12. Have you visited the alternate restoration site? If not, is it important for your team to walk through and familiarize itself with the facility?

A-2. Questions for Restoration Management Team

1. Are you familiar with the notification procedure in the Contingency Plan?
2. Identify the types of information your team will provide after a disaster has been declared:
 - Disaster declaration
 - Relocation decision
 - Operations restored
 - Recovery progress and status
3. Name the different groups and organization that your team is responsible for providing notification:
 - Contingency Plan Coordinator
 - All team leaders
 - User groups
4. Do you have valid phone numbers, fax numbers, and email addresses for all groups and organizations you will interact with?
5. How would you carry out your duties if the phone system were down?
6. How would you carry out your duties if the Internet in the building were down?
7. How would you carry out your duties if the building were evacuated? Where will you work? Do you have means to communicate at your alternate work place?
8. Are you authorized to make public announcements or respond to media inquiries?

A-3. Questions for Emergency Response Team

1. What are the team's responsibilities after a disaster has been declared?
2. Who has the authority to activate the team?
3. Does your team have the knowledge to assess damages to the IT infrastructure, system, and physical conditions of the facility?
4. Does the team have the knowledge to assess safety and health risks?
5. Does the team have the knowledge and experience to accurately predict how long it will take to complete onsite restoration?
6. Is the team comfortable to make recommendations whether or not to declare a disaster?
7. Is the team comfortable in making recommendations whether or not to order relocation?
8. When will you instruct the Contingency Plan Coordinator to contact the restoration service provider and instruct the provider to start preparing the alternate site?

A-4. Questions for Contingency Plan Coordinator/Team

1. Do you have phone numbers and email addresses for all team leaders, team members, and other appropriate personnel?
2. If the building is evacuated, how and from where will you perform your coordination duties? Do you have a “command center” from which you can operate under such conditions? Will you operate from your home?
3. If the phone system is down, how will you perform your coordination duties?
4. In what areas do you have decision-making responsibilities?
5. When will you contact the restoration service provider to start preparing the alternate site?
6. Do you communicate in any way with the user community?
7. Who is responsible for providing accommodations for the teams while at the alternate site?
8. Who is responsible for requesting that the tape storage facility send the backup tapes?
9. Who is responsible for ensuring that the correct tapes were shipped?
10. When will you instruct the Acceptance Team to get ready for testing? When will you instruct the Acceptance Team to start testing?
11. Who is responsible for declaring “Operations Restored?”
12. Who is responsible for transporting team members to the alternate site?
13. Who is responsible for making accommodation arrangements at the alternate site?

A-5. Questions for Recovery/Restoration Team

1. When was the last time you restored the entire system from backup tapes?
2. How do you know that the last backup job was completed successfully?
3. Have you ever ordered tapes from the storage facility? What is the request and approval process?
4. Who is authorized to contact the offsite storage facility and order tapes?
5. Who is authorized to call the restoration site and reserve the site?
6. If the source of the failure cannot be determined (e.g., system, host, or network), how will you work together with other Recovery/Restoration Teams to isolate and repair the problem?
7. During the restoration process, when will you be allowed to interact directly with the technical staff of the third-party provider at the restoration site?
8. Are you allowed to interact with the Restoration Site Management and request services not contracted?
9. What happens if the tape backup unit at the alternate site fails? How will you restore the data?
10. What will you do if the offsite storage facility cannot find the requested tapes or refuses to ship the tapes because they have not been paid for their services?
11. Who sets the priority of your restoration activities? Who do you report progress and concerns to?
12. What will you do if the restoration service provider failed to prepare the platform for the installation of the system? Can you install and configure the platform? Have you ever installed and configured the platform?
13. Do you have written installation and configuration procedures? Were the procedures ever tested by you personally? Were the procedures ever tested by someone else?
14. Who is responsible for IT security at the alternate site?
15. Who is responsible for physical security at the alternate site?
16. Where will you stay while working at the alternate site?
17. Can you get to the alternate site using your own means of transportation?

A-6. Questions for Acceptance Team

1. Do you have written functional test procedures to follow?
2. Do the procedures cover all system functions?
3. Who is responsible for testing the alternate site facility to ensure it is secure and that it provides the services (e.g., phone or fax) contracted?
4. Are you required to conduct the test both onsite and remotely?
5. Describe the decision process leading to a system's acceptance even though all functions were not restored?
6. How will you react to pressure from the Management Team to declare the system functional if you disagree?
7. Do you have a list of minimum functionality that will warrant acceptance?
8. How will you convey to the Management Team and user community what functions were not restored and how it will affect operations?
9. Have you tested the acceptance procedure on a restored system?
10. During the contingency plan activities, who gives you instructions and to whom do you report?

Appendix E: Example NASA Structured Walk Through Test (Simulation Testing)EXAMPLE NASA STRUCTURED WALK THROUGH TEST (SIMULATION TESTING)



<System Name>

<Organization>

**Contingency Plan
Structured Walk-Through Test
(Simulation Testing)**

Contingency Plan Structured Walk-Through Test (Simulation Testing)

1. Introduction

After system contingency plans are documented, it is critical that these plans be tested to ensure that the recovery process is not only well documented, but also understood by the staff responsible for the recovery. Several types of tests can be executed to verify if a contingency plan is viable and effective, as well as if personnel (i.e., Agency employees and third-party service providers) are well trained in all aspects of the recovery and restoration processes documented in the Contingency Plan. The Agency testing strategy calls for three testing levels—table top, simulation exercises, and alternate site. Each testing level has its own objectives and each level has increased degrees of complexity as listed below:

- **Tabletop Test**—most informal contingency testing procedure. It is designed to test the knowledge and awareness of the teams and to ensure that participants are aware of their roles and participation in the processes to recover data and systems.
- **Simulation Exercise**—more advanced test. A simulation exercise uses the existing Contingency Plan and measures its effectiveness against a fictional series of calamitous events. All responsible staff should be present at the simulation, as well as a representative from each business unit.
- **Alternate Site Test**—transfers operations to the alternate restoration facility. This test is used to ensure that the alternate site operates as planned during the recovery process and after the system has been recovered. Third-party vendors may be included in this test.

This document focuses on simulation test strategy.

***Simulation Testing: simulation testing is a role-play of the contingency test plan. The contingency testers, including all necessary operational and support personnel, role-play a disaster or disruption of service scenario prepared by a test director. The responses of the team are recorded, including measurements such as the time it takes to complete each task. The simulation may go to the point of relocating to the alternate backup site or enacting recovery procedures, but does not perform any actual recovery process or alternate processing.**

2. Simulation Objectives:

There are six objectives for simulation testing:

- Examine organizational records or documents to determine if organization reviews the contingency plan test results and takes corrective actions.
- Interview selected organizational personnel with contingency planning and plan implementation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the contingency plan testing control are documented and the resulting information to actively improve the control on a continuous basis.
- Interview selected organizational personnel with contingency planning and plan implementation responsibilities to determine the overall effectiveness of the contingency plan and the readiness of the organization to execute the plan.

-
- Verify that all Recovery/Restoration Team members understand their role in the recovery of a system. In order to meet this objective, all team members must do the following:
 - Have a copy of the latest Contingency Plan
 - Become familiar with the Contingency Plan
 - Understand the plan, anticipate the sequence of events leading to a system recovery, and know their precise individual roles and responsibilities to support an effective recovery
 - Understand how to interact with other teams that are also assisting in the recovery effort
 - Know their own team members, as well as other team leads
 - Keep in their possession, both onsite and offsite, the pertinent information needed to perform their recovery duties
 - Have the media, other materials, and tools needed to ensure an effective recovery
 - Resolve all questions and ambiguities during the table top test
 - Improve the Contingency Plan by modifying the plan based on discussions, observations, and findings identified during the simulation test.
 - Provide Agency's management and team leads with a test summary. This summary, prepared by the test director, should outline successes and areas for improvement.

3. Test Assumptions

The following assumptions are made, which were specifically designed for the simulation test, to ensure that the test is effective:

- For this simulation the assumption is that there is NOT a local, regional, or natural disaster and the network is up and running.
- The test will take place after individual contingency plans have been completed.
- The test will take place even if some team members cannot attend, which simulates actual situations that may occur during an emergency.
- The organization has officially assigned well-suited individuals to the various Recovery/Restoration Teams. The position description for individuals participating in the contingency operations was updated to reflect their assigned responsibilities.
- All team members have a copy of the Contingency Plan and its appendices, have read the plan, and have an understanding of their team roles, as well as the roles of teams with whom they interact.
- All team members will bring their personal copy of the plan to the test and refer to it when needed.
- All participants are cleared to enter the facility and the conference room for testing.

4. Test Scope X

The scope of the Structured Walk Through Test consists of a verbal acknowledgement by team members of their recovery and restoration responsibilities, as well as a demonstration of their knowledge of the recovery process and their specific duties within this process. The test is limited to questions (presented by the test director), answers (by team members). Team

members are encouraged to ask the director for clarifications when ambiguous points and issues are discussed.

The scope does not include any hands-on use of equipment that is used during an actual recovery (e.g., phone system, tape backup unit, server, and router). The scope does not include a walk-through of the alternate relocation site.

The test is limited to the system covered by the Contingency Plan. A disaster may affect infrastructure components for which members have no restoration responsibilities. In future tests, when an infrastructure component (e.g., air conditioning [AC], electricity, or network) failure brings down the system under consideration, the test should include demonstrating an understanding of how the Recovery/Restoration Team will interact with recovery personnel involved in the facility restoration process.

5. Roles and Responsibilities

The Contingency Plan identifies the teams listed below as instrumental in the recovery from an emergency. Specific contingency plans may include some of these teams, all of these teams or additional teams the contingency planning groups may consider necessary. The Simulation test includes only those teams listed in the system's Contingency Plan.

Contingency Plan Work Group

The Contingency Plan Work Group completes all preliminary activities, including agreements for offsite storage and space at the alternate operating facilities. The Work Group supports the Contingency Coordinator in developing strategies to keep the organization's critical Information Technology (IT) functions operational.

Restoration Management Team

The Restoration Management Team has the overall responsibility for handling the disaster (after a disaster has been declared) and deciding the best course of action needed to restore operations both onsite and offsite.

Emergency Response Team

The Emergency Response Team is responsible for assessing the overall adverse event's impact on safety, health, and operations, as well as predicting how long it will take (if possible) before full recovery can be achieved onsite. The team's *Damage Assessment Report* will be used by the Restoration Management Team to decide whether to relocate operations to the alternate site.

Contingency Coordination Team

The Contingency Coordinator is the focal point for conveying instructions from the Restoration Management Team to team leaders and for disseminating status information to all team leaders. The Coordinator is supported by an appropriate size team.

Recovery/Restoration Team

The Recovery/Restoration Team has the overall responsibility for restoring the system to its full/partial capabilities, whether onsite or offsite, as instructed by the Restoration Management Team.

Acceptance Team

The Acceptance Team has the overall responsibility for the functional testing of the restored system and then accepting or rejecting it. Acceptance of limited capabilities must be justified to

the Restoration Management Team. The actual declaration that a system is fully or partially restored is made by the Restoration Management Team.

6. Success Criteria

- To ensure that the plan accurately reflects the organizations ability to recovery application software in the event of a disruption.
- Minimize the effects that the disaster would have on the organization.
- To ensure that resources, personnel and business processes are able to resume in a timely manner.
- To ensure that all personnel know their roles in the contingency plan process.
- To find gaps in the contingency plan and improve upon the contingency plan process for the organization.
- Minimize threats, impacts and down-time to mitigate any losses.

The test will be considered a success if all its objectives, as listed in Section 2 and 6, were met and if the test director determines that all participants have sufficient knowledge of the plan, their roles and responsibilities, and the means needed to perform their recovery duties effectively. The test report, developed by the director after the test is completed, will identify the perceived level of success, as well as recommendations for improvements.

7. Test Logistics

There are few logistical test requirements because no actual or simulated hardware will be used during the simulation test. There will be however a simulated application failure and software recovery. Computer hardware, software, tools, supplies, meals, and beverages are not needed. Other test logistics include:

- Schedule—test is scheduled to last <two> hours. Exact dates and times will be coordinated with all participants by the Contingency Coordinator.
- Facility—team members must be present for this test—they cannot participate via a conference call.
- Communications—projector is needed; however no computer equipment is needed—director will bring own laptop.

8. Technical and Business Impacts

Simulation testing does not impact a system's operational status or the user community; however, there may be some impact on the support level for the system since many participants are responsible for the system's operation and support. It is the system owner's responsibility to verify that a sufficient level of user and technical support is maintained during the testing period.

9. Test Activities

This section contains a scenario to be used during the simulation testing. The disaster scenario will be presented to the participants and questions specific to the scenario presented will be asked (see Appendix A).

Scenario:

Your application has suddenly failed. You have placed a call to the help desk and the technicians have determined that the problem is not workstation or communication related. The technicians have found your database code has been corrupted and your application is not functioning. Describe the process you would employ to restore your application to functional status.

Note: The test may be stopped by the director if a determination is made that participants do not have sufficient knowledge or an understanding of the Contingency Plan.

A-1. Questions for Table Top - Simulation Testing

Appendix A consists of the list of questions asked to all team members, as well as specific teams, during the table top part of the test. It includes questions for the following:

- All Team Members
- Restoration Management Team
- Emergency Response Team
- Contingency Coordination Team
- Recovery/Restoration Team
- Acceptance Team

A.2. Questions for All Team Members – Simulation Testing

1. Have you brought your copy of the plan?
2. Do you have a copy of the plan at home in case a disaster is declared after hours or a building emergency evacuation is ordered?
3. Have you read the plan?
4. How would you be notified that a disaster has been declared?
5. Do you have instructions on what to do if the phone network is down and the building has been evacuated? Where will you work from if the building is evacuated for a prolonged period?
6. Can you name the team members that support contingency activities for your system?

A-3. Questions for Restoration Management Team – Simulation Testing

1. Are you familiar with the notification procedure in the Contingency Plan?
2. Identify the types of information your team will provide after a disaster has been declared:
 - Disaster declaration
 - Relocation decision
 - Operations restored
 - Recovery progress and status
3. Do you have valid phone numbers, fax numbers, and email addresses for all groups and organizations you will interact with?
4. How would you carry out your duties if the building were evacuated? Where will you work? Do you have means to communicate at your alternate work place?

A-4. Questions for Emergency Response Team – Simulation Testing

1. What are the team's responsibilities after a disaster has been declared?
2. Who has the authority to activate the team?
3. Is the team comfortable to make recommendations whether or not to declare a disaster?
4. Is the team comfortable in making recommendations whether or not to order relocation?
5. When will you instruct the Contingency Plan Coordinator to contact the restoration service provider and instruct the provider to start preparing the alternate site?

A-5. Questions for Contingency Plan Coordinator/Team – Simulation Testing

1. Do you have phone numbers and email addresses for all team leaders, team members, and other appropriate personnel?
2. When will you contact the restoration service provider to start preparing the alternate site?
3. Who is responsible for requesting that the tape storage facility send the backup tapes?
4. Who is responsible for declaring “Operations Restored”?

A-6. Questions for Recovery/Restoration Team – Simulation Testing

1. Who is authorized to make the decision to restore to a previous version of your software
2. Who is authorized to contact the offsite storage facility and order tapes?
3. What happens if the tape backup unit at the alternate site fails? How will you restore the data?
4. At what point would you consider a restoration from PVCS of a previous version of your software.
5. Who is authorized to call the restoration site and reserve the site?
6. Who sets the priority of your restoration activities? Who do you report progress and concerns
7. Do you have written installation and configuration procedures? Were the procedures ever tested by you personally? Were the procedures ever tested by someone else?

A-7. Questions for Acceptance Team – Simulation Testing

1. Do you have written functional test procedures to follow?
2. Do the procedures cover all system functions?
3. Describe the decision process leading to a system's acceptance even though all functions were not restored?
4. Do you have a list of minimum functionality that will warrant acceptance?
5. During the contingency plan activities, who gives you instructions and to whom do you report?