ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

CONTINGENCY PLANNING GUIDE FOR INFORMATION TECHNOLOGY SYSTEMS

Elizabeth B. Lennon (Editor)
Information Technology Laboratory
National Institute of Standards and Technology

Information technology (IT) and automated information systems are vital elements in most business processes. Because these IT resources are so essential to an organization's success, it is critical that the services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement 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. Interim measures may include the relocation of IT systems and operations to an alternate site, the recovery of IT functions using alternate equipment, or the performance of IT functions using manual methods.

NIST's Information Technology Laboratory has published a recommended guidance document on contingency planning for federal departments and agencies. (Industry will find the recommendations valuable as well.) NIST Special Publication (SP) 800-34, *Contingency Planning Guide for Information Technology Systems*, by Marianne Swanson, Amy Wohl, Lucinda Pope, Tim Grance, Joan Hash, and Ray Thomas, provides instructions, recommendations, and considerations for government IT contingency planning. NIST SP 800-34 supersedes Federal Information Processing Standard (FIPS) 87, Guidelines for ADP Contingency Planning.

NIST SP 800-34 provides guidance to individuals responsible for preparing and maintaining IT contingency plans. The guide discusses essential contingency plan elements and processes, highlights specific considerations and concerns associated with contingency planning for various types of IT systems, and provides examples to assist readers in developing their own IT contingency plans. This *ITL Bulletin* summarizes the contingency planning guide, which is available at http://csrc.nist.gov/publications/nistpubs/index.html.

Fundamental Contingency Planning Principles

The IT contingency planning guide identifies fundamental planning principles and practices to help personnel develop and maintain effective IT contingency plans. The principles meet most organizational needs; however, each organization may have additional requirements specific to its own processes. The document provides guidance to help personnel evaluate information systems and operations to determine contingency requirements and priorities. The guidance also provides a structured approach to aid planners in developing cost-effective solutions that accurately reflect their IT requirements and integrate contingency planning principles into all aspects of IT operations.

The guidance presented should be considered during every stage of contingency planning, starting with the conceptualization of contingency planning efforts through plan maintenance and disposal of the contingency plan. If used as a planning management tool throughout the contingency planning process, the document and its appendices should provide users with time- and cost-saving practices.

Scope

The guide presents contingency planning principles for the following common IT processing systems:

- Desktop computers and portable systems (laptop and handheld computers)
- Servers

Continued on page 2

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. **Bulletins are issued on an as-needed basis** and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8901, Gaithersburg, MD 20899-8901, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since October 2000

- Websites
- Local area networks (LANs)
- Wide area networks (WANs)
- Distributed systems
- Mainframe systems.

The document discusses common technologies that may be used to support contingency capabilities. Given the broad range of IT designs and configurations, however, as well as the rapid development and obsolescence of products and capabilities, the scope of the discussion is not intended to be comprehensive. Rather, the document describes practices for applying technology to enhance an organization's IT contingency planning capabilities.

The document outlines planning principles that may be applied to a wide variety of incidents that could affect IT system operations. The scope includes minor incidents causing short-term disruptions to disasters that affect normal operations for an extended period. Because IT systems vary in design and application, specific incident types and associated contingency measures are not provided in the document. Instead, the planning guide defines a process that may be followed for any IT system to identify planning requirements and develop an effective contingency plan.

Audience

Managers within federal organizations and those individuals responsible for IT security at system and operational levels can use the principles presented in the document. This description includes the following personnel:

- *Managers* responsible for overseeing IT operations or business processes that rely on IT systems;
- *System administrators* responsible for maintaining daily IT operations;
- *Information System Security Officers (ISSOs)* and other staff responsible for developing, implementing, and maintaining an organization's IT security activities;
- *System engineers and architects* responsible for designing, implementing, or modifying information systems;
- *Users* who employ desktop and portable systems to perform their assigned job functions; and
- *Other personnel* responsible for designing, managing, operating, maintaining, or using information systems.

In addition, emergency management personnel who may need to coordinate facility-level contingency may use this document with IT contingency planning activities. The concepts presented in this document are not specific to government systems and may be used by private and commercial organizations.

Risk Management Process

IT systems are vulnerable to a variety of disruptions, ranging from mild (e.g., short-term power outage, disk drive failure) to severe (e.g., equipment destruction, fire). Many vulnerabilities may be minimized or eliminated through technical, management, or operational solutions as part of the organization's risk management effort; however, it is virtually impossible to completely eliminate all risks. Contingency planning is designed to mitigate the risk of system and service unavailability by focusing effective and efficient recovery solutions.

NIST SP 800-34 discusses the ways in which IT contingency planning fits into an organization's larger risk management, security, and emergency preparedness programs. Other types of emergency-related plans and their relationship to IT contingency planning are described. Finally, the guide explains how integrating contingency planning principles throughout the system development life cycle promotes system compatibility and a cost-effective means to increase an organization's ability to respond quickly and effectively to a disruptive event.

IT Contingency Planning Process

To develop and maintain an effective IT contingency plan, organizations should use the following approach:

1. Develop the contingency planning policy statement
2. Conduct the business impact analysis (BIA)
3. Identify preventive controls
4. Develop recovery strategies
5. Develop an IT contingency plan
6. Plan testing, training, and exercises
7. Plan maintenance.

These steps represent key elements in a comprehensive IT contingency planning capability. The responsibility for the planning process generally falls under the auspice of the "Contingency Planning Coordinator" or "Contingency Planner," who is typically a functional or resource manager within the agency. The coordinator develops the strategy in cooperation with other functional and resource managers associated with the system or the business processes supported by the system. The Contingency Planning Coordinator also typically manages development and execution of the contingency plan. All major applications and general support systems should have a contingency plan.

1. Develop the contingency planning policy statement. To be effective and to ensure that personnel fully understand the agency's contingency planning requirements, the contingency plan must be based on a clearly defined policy. The contingency planning policy statement should define the agency's overall contingency objectives and establish the organizational framework and responsibilities for IT contingency planning. To be successful, senior management, most likely the Chief Information Officer (CIO), must support a contingency program. These officials

ITL Bulletins Via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.

should be included in the process to develop the program policy, structure, objectives, and roles and responsibilities. At a minimum, the contingency policy should comply with federal guidance contained in the documents listed in NIST SP 800-34; agencies should evaluate their respective IT systems, operations, and requirements to determine if additional contingency planning requirements are necessary. Key policy elements are as follows:

- Roles and responsibilities
- Scope as applies to the type(s) of platform(s) and organization functions subject to contingency planning
- Resource requirements
- Training requirements
- Exercise and testing schedules
- Plan maintenance schedule
- Frequency of backups and storage of backup media.

2. Conduct the business impact analysis (BIA). The BIA is a key step in the contingency planning process. The BIA enables the Contingency Planning Coordinator to fully characterize the system requirements, processes, and interdependencies and use this information to determine contingency requirements and priorities. The purpose of the BIA is to correlate specific system components with the critical services that they provide, and based on that information, to characterize the consequences of a disruption to the system components. Key steps are listing critical IT resources, identifying disruption impacts and allowable outage times, and developing recovery priorities.

Results from the BIA should be appropriately incorporated into the analysis and strategy development efforts for the organization's other continuity and recovery plans. NIST SP 800-34 provides a sample BIA process, which helps Contingency Planning Coordinators streamline and focus their contingency plan development activities to achieve a more effective plan.

3. Identify preventive controls. In some cases, the outage impacts identified in the BIA may be mitigated or eliminated through preventive measures that deter, detect, and/or reduce impacts to the system. Where feasible and cost-effective, preventive methods are preferable to actions that may be necessary to recover the system after a disruption. 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. A variety of preventive controls are available, depending on system type and configuration; however, some common measures are listed below:

- Appropriately sized uninterruptible power supplies (UPS) to provide short-term backup power to all system components (including environmental and safety controls)
- Gasoline- or diesel-powered generators to provide long-term backup power
- Air-conditioning systems with adequate excess capacity to permit failure of certain components, such as a compressor
- Fire suppression systems
- Fire and smoke detectors
- Water sensors in the computer room ceiling and floor
- Plastic tarps that may be unrolled over IT equipment to protect it from water damage
- Heat-resistant and waterproof containers for backup media and vital nonelectronic records
- Emergency master system shutdown switch
- Offsite storage of backup media, nonelectronic records, and system documentation
- Technical security controls, such as cryptographic key management and least-privilege access controls
- Frequent, scheduled backups.

4. Develop recovery strategies. Recovery strategies provide a means to restore IT operations quickly and effectively following a service disruption. 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 contingency plans.

The selected recovery strategy should address the potential impacts identified in the BIA and should be integrated into the system architecture during the design and implementation phases of the system life cycle.

The strategy should include a combination of methods that complement one another to provide recovery capability over the full spectrum of incidents. A wide variety of recovery approaches may be considered; the appropriate choice depends on the incident, type of system, and its operational requirements. Specific recovery methods may include commercial contracts with cold, warm, or hot site vendors, mobile sites, mirrored sites, reciprocal agreements with internal or external organizations, and service level agreements (SLAs) with the equipment vendors. In addition, technologies such as Redundant Arrays of Independent Disks (RAID), automatic fail-over, uninterruptible power supply (UPS), and mirrored systems should be considered when developing a system recovery strategy.

5. Develop an IT Contingency Plan. IT contingency plan development is a critical step in the process of implementing a comprehensive contingency planning program. The plan contains detailed roles, responsibilities, teams, and procedures associated with restoring an IT system following a disruption. The contingency plan should document technical capabilities designed to support contingency operations. The contingency plan should be tailored to the organization and its requirements. Plans need to balance detail with flexibility; usually the more detailed the plan, the less scalable and versatile the approach. The information presented in NIST SP 800-34 is meant to be a guide; however, the plan format may be modified as needed to better meet the user's specific system, operational, and organization requirements.

In our approach, the contingency plan comprises five main components: *Supporting Information, Notification/Activation, Recovery, Reconstitution,* and *Plan Appendices*. The first and last components provide essential information to ensure a comprehensive plan. The Notification/Activation, Recovery, and Reconstitution phases address specific actions that the organization should take following a system disruption or emergency.

- The Supporting Information component includes an introduction and concept of operations section that provides essential background or contextual information that makes the contingency plan easier to understand, implement, and maintain. These details aid in understanding the applicability of the guidance, in making decisions on how to use the plan, and in providing information on where associated plans and information outside the scope of the plan may be found.
- The Notification/Activation Phase defines the initial actions taken once a system disruption or emergency has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, assess system damage, and implement the plan. At the completion of the Notification/Activation Phase, recovery staff will be prepared to perform contingency measures to restore system functions on a temporary basis.
- The Recovery Phase begins after the contingency plan has been activated, damage assessment has been completed (if possible), personnel have been notified, and appropriate teams have been mobilized. Recovery phase activities focus on contingency measures to execute temporary IT processing capabilities, repair damage to the original system, and restore operational capabilities at the original or new facility. At the completion of the Recovery Phase, the IT system will be operational and performing the functions designated in the plan. Depending on the recovery strategies defined in the plan, these functions could include temporary manual processing, recovery and operation on an alternate system, or relocation and recovery at an alternate site. Teams with recovery responsibilities should understand and be able to perform these recovery strategies well enough that if the paper plan is unavailable during the initial stages of the event, they can still perform the necessary activities.
- In the Reconstitution Phase, recovery activities are terminated, and normal operations are transferred back to the organization's facility. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new facility to support system processing requirements. Once the original or new site is restored to the level that it can support the IT system and its normal processes, the system may be transitioned back to the original or to the new site. Until the primary system is restored and tested, the contingency system should continue to be operated. The Reconstitution Phase should specify teams responsible for restoring or replacing both the site and the IT system.
- Contingency Plan Appendices provide key details not contained in the main body of the plan. The appendices should reflect the specific technical, operational, and management contingency requirements of the given system. Appendices can include, but are not limited to contact information for contingency planning team personnel; vendor contact information, including offsite storage and alternate site POCs; standard operating procedures and checklists for system recovery or processes; equipment and system requirements lists of the hardware, software, firmware, and other resources required to support system operations; vendor agreements, reciprocal agreements with other organizations, and other vital records; description of, and directions to, the alternate site; and the BIA.

Plans should be formatted to provide quick and clear direction in the event those personnel unfamiliar with the plan or the systems are called on 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 creating an overly complex or confusing plan.

6. Plan Testing, Training, and Exercises. Plan testing is a critical element of a viable contingency capability. Testing enables plan deficiencies to be identified and addressed. Testing also helps evaluate the ability of the recovery staff to implement the plan quickly and effectively. Each IT contingency plan element should be tested to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan. The following areas should be addressed in a contingency test:

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

Training for personnel with contingency plan responsibilities should complement testing. Training should be provided at least annually; new hires

with plan responsibilities should receive training shortly after they are hired. Ultimately, contingency plan personnel should be trained to the extent that 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 of the plan
- Cross-team coordination and communication
- Reporting procedures
- Security requirements
- Team-specific processes (Notification/Activation, Recovery, and Reconstitution Phases)
- Individual responsibilities (Notification/Activation, Recovery, and Reconstitution Phases).

7. Plan Maintenance. To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. IT systems undergo frequent changes because of shifting business needs, technology upgrades, or new internal or external policies. Therefore, it is essential that the contingency plan be reviewed and updated regularly, as part of the organization's change management process, to ensure new information is documented and contingency measures are revised if required. As a general rule, the plan should be reviewed 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 reasonable to evaluate plan contents and procedures more frequently.

Following the step-by-step guidance on the contingency planning process, NIST SP 800-34 contains an in-depth discussion of technical contingency planning considerations for specific types of IT systems. Eight appendices complete the document. Appendices give sample formats, address frequently asked questions, discuss human factors, and present a glossary, suggested resources, references, and an index.

NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, presents an efficient and cost-effective approach for federal agencies to develop policies and procedures for the timely recovery and restoration of critical IT processes and vital government services to the public.

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900