# ITL BULLETIN FOR JULY 2010

## CONTINGENCY PLANNING FOR INFORMATION SYSTEMS: UPDATED GUIDE FOR FEDERAL ORGANIZATIONS

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Interruptions to information technology (IT) system services can have a severe impact on an organization and its ability to carry out its basic functions. IT resources are essential to most business processes, and organizations depend upon information systems that operate effectively without serious interruptions. When organizations develop and maintain contingency plans for their IT systems, they can create a coordinated strategy to identify technical procedures and methods that will prevent most service disruptions and enable quick recovery should any disruptions occur.

The Information Technology Laboratory of the National Institute of Standards and Technology (NIST) recently issued an updated guide to effective contingency planning practices, replacing an earlier guide that had been issued in 2002. NIST Special Publication (SP) 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems,* updates federal contingency planning practices by integrating risk management and system development life cycle (SDLC) considerations into the contingency planning process.

### NIST Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*

NIST SP 800-34, Rev.1, provides instructions, recommendations, and considerations to assist federal organizations in developing and maintaining effective contingency plans. The guide covers contingency planning principles for three types of system platforms: client/server systems, telecommunications systems, and mainframe systems. Strategies and techniques common to these systems, and a defined process for identifying planning requirements, are discussed. The authors are Marianne Swanson and Pauline Bowen (retired) of NIST, and Amy Wohl-Phillips, Dean Gallup, and David Lynes of Booz Allen Hamilton.

The guide explains the ways in which contingency planning fits into an organization's risk management, security, and emergency preparedness programs and plans, and how these programs and plans are related to contingency planning. Also discussed is the integration of contingency planning principles throughout the system development life cycle to promote system compatibility and a cost-effective means for responding quickly and effectively to a disruptive event.

Other sections of the guide detail the information system contingency planning process, the steps in the development of contingency plans, and the technical considerations that pertain to the three types of system platforms that are covered.

Comprehensive appendices provide additional help to organizations in their contingency planning activities. The appendices include templates for contingency plans for systems that have been categorized as low-impact, moderate-impact, and high-impact systems (as required by Federal Information Processing Standard [FIPS] 199, *Standards for Security Categorization of Federal Information and Information Systems*); a template to assist organizations in conducting a Business Impact Analysis (BIA) for a system; answers to frequently asked questions about contingency planning; considerations for the health, safety, and well-being of personnel to be included in an organization's contingency planning; a summary of the technical, operational, and management controls that apply to contingency planning; and the relationship of contingency planning to the SDLC. A glossary, a list of acronyms, and references to additional resources on contingency planning are provided.

NIST SP 800-34, Rev. 1, is available from the NIST Web page http://csrc.nist.gov/publications/PubsSPs.html.

**Contingency Planning, Risk Management, and the System Development Life Cycle**

Contingency planning is an integral component of the federal government's risk management policies and its practices for incorporating security into all phases of the system development life cycle.

The Federal Information Security Management Act (FISMA) of 2002 establishes a governmentwide policy for the implementation and assessment of security controls. FISMA requires that federal agencies develop, document, and implement programs to protect their information and information systems. This policy applies to the systems that support the operations and assets of the agency, and includes those systems provided or managed by another agency, contractor, or other source. FISMA calls for agencies to apply a risk-based policy to achieve cost-effective results for the security of their information and information systems.

Standards and guidelines developed by NIST help agencies to carry out effective information security programs based on the management of risk. FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, specifies that federal organizations categorize their information and information systems as low-impact, moderate-impact, or high-impact systems for the following security objectives:

- Confidentiality – releasing information only to those authorized to have it;
- Integrity – ensuring that information is not changed or destroyed; and
- Availability – being able to access information when it is needed.

The categorization is based on the potential impact on the organization should disruptive events occur to jeopardize the information and information systems needed by the organization to accomplish its mission and carry out its responsibilities.

Under FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, federal organizations specify minimum security requirements to protect the confidentiality, integrity, and availability of their information systems and the information processed, stored, and transmitted by those systems, based on the impact levels that they have determined.

For each information system, agencies select an appropriate set of security controls to satisfy minimum security requirements from NIST SP 800-53, Rev. 3, *Recommended Security Controls for Federal Information System and Organizations*, using a risk-based approach. Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. NIST SP 800-53A, Rev. 1, *Guide for Assessing the Security Controls in Federal Information Systems*, provides procedures for assessing the effectiveness of controls.

NIST developed the Risk Management Framework (RMF) to guide agencies through a structured process to identify the risks to the information systems, assess the risks, and take steps to reduce risks to an acceptable level, and recently issued NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.* See the following NIST Web page for information about the RMF: http://csrc.nist.gov/groups/SMA/fisma/framework.html.

The risk-based approach to the management of information systems is most effective when integrated into the organization's strategic planning processes. Risk management tasks should begin during the system initiation phase when the security capabilities of the system are determined. NIST SP 800-37, Rev. 1, provides a link for each step in the Risk Management Framework to the appropriate phase of the SDLC to assure that information security considerations are addressed as early as possible and that security controls are implemented to mitigate risks. Contingency planning principles should also be integrated into the SDLC. This practice will enable organizations to promote system compatibility and to respond quickly and effectively to disruptive events.

**The Contingency Planning Process**

Contingency planning is the process for establishing plans, procedures, and technical measures to recover information system services after a disruption. Interim measures to be considered include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods. Contingency planning for a system is unique to that system; the planning process provides preventive measures, recovery strategies, and technical considerations that are appropriate to the organization's

requirements to protect the confidentiality, integrity, and availability of information at the established FIPS 199 impact level.

The planning process includes designing a contingency planning program; evaluating the organization's needs against contingency strategy options based on the FIPS 199 impact levels; selecting security controls; and documenting the contingency strategy into a contingency plan, testing the plan, and maintaining it. The completed and maintained plan should contain detailed specific guidance to enable staff members to react effectively in the event of a disruption.

NIST recommends that organizations follow a seven-step process in developing and maintaining a contingency planning program for their information systems. These seven progressive steps are designed to consider risk management principles and the integration of security into each stage of the system development life cycle.

• **Develop the contingency planning policy statement.** A formal policy provides the authority and guidance necessary to develop an effective contingency plan. The contingency planning policy statement should define the organization's overall contingency objectives and establish the organizational framework and responsibilities for system contingency planning. The inclusion of senior management in the development of the program policy helps to assure support for the contingency program. The policy should reflect the FIPS 199 impact levels and the controls required for each established impact level.

• **Conduct the business impact analysis (BIA).** The BIA helps to identify and prioritize information systems and components critical to supporting the organization's mission and business functions. The BIA enables the organization to characterize the system components, identify the mission and business functions that are supported, and determine their interdependencies. With this information, organizations can then characterize the consequences of a disruption. The BIA results can be used to determine contingency planning requirements and priorities. Results from the BIA should be appropriately incorporated into the organization's other emergency planning activities.

• **Identify preventive controls.** Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs. In some cases, the impact of system disruptions identified in the BIA may be mitigated or eliminated through preventive measures that deter, detect, and 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. The Risk Management Framework (RMF) includes a step to identify effective contingency planning preventive controls and to maintain the controls on an ongoing basis. NIST SP 800-53, Rev. 3, identifies preventive controls such as using uninterruptible power supplies, generators, fire protection systems, and smoke detectors.

• **Create contingency strategies.** Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption. Organizations are

guided by the RMF, FIPS 199, and NIST SP 800-53, Rev. 3, in selecting and implementing the right set of security controls. The contingency planning family of controls covers the full range of backup, recovery, contingency planning, testing, and ongoing maintenance activities. Backup and recovery methods and strategies provide a means to restore system operations quickly and effectively following a service disruption. The methods and strategies should address disruption impacts and allowable downtimes identified in the BIA and should be integrated into the development and acquisition phase of the system life cycle.

• **Develop an information system contingency plan.** The contingency plan should contain detailed guidance and procedures for restoring an information system following a disruption. The development of the contingency plan is the key step in implementing a comprehensive contingency planning program. The plan contains detailed roles, responsibilities, teams, and procedures and includes technical information designed to support contingency operations that are tailored to the organization, information system, and its requirements. Plans should balance detail with flexibility; usually, the more detailed the plan, the less scalable and versatile the approach.

The guide presents three sample formats for developing an information system contingency plan based on low-, moderate-, or high-impact levels, as defined by FIPS 199. Each format defines three phases that govern actions to be taken following a system disruption:

· **Activation/Notification Phase** describes the process of activating the plan based on outage impacts and notifying recovery personnel.

· **Recovery Phase** details a suggested course of action for recovery teams to restore system operations at an alternate site or using contingency capabilities.

· **Reconstitution Phase** includes activities to test and validate system capability and functionality and outlines actions that can be taken to return the system to normal operating condition and prepare the system against future outages.

• **Ensure plan testing, training, and exercises.** Testing is a critical element of a contingency program. Testing enables plan deficiencies to be identified and addressed by validating one or more of the system components and the operability of the plan. Testing can take on several forms and accomplish several objectives but should be conducted in as close to an operating environment as possible. Each information system component should be tested to confirm the accuracy of individual recovery procedures.

Training for personnel with contingency plan responsibilities should focus on familiarizing them with the contingency planning roles and teaching skills necessary to accomplish those roles. This approach helps ensure that the staff is prepared to participate in tests and exercises as well as actual outage events. Training should be provided at least annually. Personnel newly appointed to contingency planning roles should receive training soon after their appointments. All contingency planning personnel should be

trained so that they are able to carry out their recovery roles and responsibilities without aid of the planning document. This is important if the plan is not available for the first few hours after the disruption.

NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for Information Technology Plans and Capabilities*, provides guidelines on designing, developing, conducting, and evaluating test, training, and exercise (TT&E) events so that organizations can improve their ability to prepare for, respond to, manage, and recover from adverse events.

Organizations should conduct TT&E events periodically, following organizational or system changes, or the issuance of new TT&E guidance, or as otherwise needed. TT&E activities help organizations determine the plan's effectiveness, and help all personnel know what their roles are in the conduct of each information system contingency plan.

• **Ensure plan maintenance.** The plan should be a living document that is updated regularly to remain current with system enhancements and organizational changes. To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. Information systems may undergo frequent changes during their operation and maintenance phases because of shifting business needs, technology upgrades, or new internal or external policies. The contingency plan should be reviewed and updated regularly, as part of the organization's change management process, to ensure that new information is documented and contingency measures are revised if necessary. The RMF identifies the continuous monitoring process as an effective tool for plan maintenance, producing ongoing updates to security plans, security assessment reports, and plans of action and milestone documents.

**For More Information**

NIST publications that provide information and guidance on planning and implementing information system security include:

Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*
FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
NIST Special Publication (SP) 800-18, *Guide for Developing Security Plans for Federal Information Systems*
NIST SP 800-30, *Risk Management Guide for Information Technology Systems*
NIST SP 800-37, Rev.1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*
NIST SP 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*

NIST SP 800-53A, Rev. 1, *Guide for Assessing the Security Controls in Federal Information Systems*
NIST SP 800-60, Rev. 1, *Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices*
NIST SP 800-61, Rev. 1, *Computer Security Incident Handling Guide*
NIST SP 800-64, Rev. 2, *Security Considerations in the System Development Life Cycle*
NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*

For information about these NIST standards and guidelines, as well as other security-related publications, see NIST's Web page http://csrc.nist.gov/publications/index.html. Information about NIST's information security programs is available from the Computer Security Resource Center at http://csrc.nist.gov/.

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.