ITL BULLETIN FOR OCTOBER 2012

CONDUCTING INFORMATION SECURITY-RELATED RISK ASSESSMENTS: UPDATED GUIDELINES FOR COMPREHENSIVE RISK MANAGEMENT PROGRAMS

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

Organizations depending upon information systems to carry out their missions and business functions are challenged by serious threats that can exploit both known and unknown vulnerabilities in systems. Threats include targeted attacks, operational disruptions due to natural disasters, human and system errors, and structural failures. These potentially harmful activities can compromise the confidentiality, integrity, or availability of information being processed, stored, or transmitted by information systems, resulting in adverse impacts on the organization, its operations, assets, and people, and endangering other organizations and national interests.

People at all levels within an organization have a role in managing information security risks to the organization's missions and business functions and the information systems that support those missions/business functions. Managing risk is a comprehensive and complex process that involves many activities and functions of an organization – its programs, investments, budgets, legal and safety issues, inventory and supply chain matters, and security. An integrated approach to managing risk brings together the best collective judgments of individuals and groups within the organization who are responsible for strategic planning, oversight, management, and day-to-day operations.

Managing Information Security Risk

Federal government organizations are directed by the Federal Information Security Management Act (FISMA) of 2002, and other legislative and executive directives, to develop, document, and implement programs to protect their information and information systems, and to apply a risk-based policy to achieve cost-effective security. Standards and guidelines developed by the National Institute of Standards and Technology (NIST) help agencies to carry out effective information security programs based on the management of risk.

The Information Technology Laboratory (ITL) at NIST has developed a risk management process and supporting Risk Management Framework (RMF) to assist organizations in applying a disciplined and structured process that integrates information security and risk management activities into the life cycle of an information system as well as other mainstream organizational management and business processes. A guide issued last year, NIST Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View,* discusses the overall risk management process and provides a structured approach for managing risk that is supported by NIST standards and guidelines. A new guide, NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*, supplements SP 800-39 and discusses risk assessments as part of an integrated approach to organization-wide risk management. See the **For More Information** section below for details about NIST's risk management publications and the RMF.

NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*

NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments,* is the fifth in the series of risk management and information security guidelines that was developed by the Joint Task Force Transformation Initiative Interagency Working Group, a partnership among the Department of Defense, the Intelligence Community, NIST, and the Committee on National Security Systems. The partnership, under the leadership of the Secretary of Defense, the Director of National Intelligence, and the Secretary of Commerce, is collaborating on the development of a unified information security framework for the federal government to address the challenges of protecting federal information and information systems as well as the Nation's critical information infrastructure. A common foundation for information security will also provide a strong basis for reciprocal acceptance of security assessments and will facilitate information sharing.

SP 800-30 Revision 1 discusses the risk management process and how risk assessments are an integral part of that process. The publication provides guidance for federal agencies in conducting risk assessments of information systems and organizations for each of the steps in the risk assessment process: preparing for the assessment, conducting the assessment, communicating the results of the assessment, and maintaining the assessment. Other topics covered in the guide include how risk assessments and other organizational risk management processes complement and support each other; how to identify specific risk factors that should be monitored on an ongoing basis; how to determine if the organization's risks have increased

to unacceptable levels; and whether different courses of action should be taken by the organization.

The appendices to the guide provide extensive additional information to assist organizations in conducting risk assessments including: general references; a glossary of terms used; acronyms; descriptions of threat sources, threat events, vulnerabilities and predisposing conditions; methods and templates for assessing, summarizing, and documenting threat sources, events, and vulnerabilities; descriptions of and scales for measuring the likelihood of occurrence of threat events; inputs to reports for determining the impact of threat events on the organization and others; descriptions and methods for summarizing and documenting the results of the risk determinations; ways to present the risk assessment results and to report on the risk assessment process; information elements for communicating the results of risk assessments; and a summary of risk assessment tasks. NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments,* is available here.

Risk Assessment as a Component of Risk Management

Risk assessment is one of the fundamental components of an organization's risk management process. NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, which provides a structured, yet flexible approach for managing risk, discusses the basic concepts of risk management with four components:

- How organizations **frame risk**, and the context in which risk-based decisions are made;
- How organizations **assess risk** within that context;
- How organizations **respond to risk** after assessment is made; and
- How organizations **monitor risk** over time.

Risk assessments help organizations identify, estimate, and prioritize risk to their operations, assets, and people, and to other organizations and national interests, resulting from the operation and use of their information systems. Risk assessments also inform decision makers and enable them to provide appropriate risk responses[1] by identifying:

[1] Risk Responses include decisions and activities associated with accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.

- Relevant threats to organizations or threats directed through organizations against other organizations;
- Vulnerabilities both internal and external to organizations;
- Harmful impacts that may occur as a result of potential threats exploiting vulnerabilities; and
- Likelihood that harm will occur.

The risk assessment process provides organizational decision makers with a determination of risk that is based on potential harm and the likelihood of harm occurring.

Risk assessments can be conducted at the three tiers in the risk management hierarchy described in SP 800-39:

• Tier one, **organization level --** addressing risk by establishing and implementing governance structures that are consistent with the strategic goals and objectives of organizations and the requirements defined by federal laws, directives, policies, regulations, standards, missions and business functions;

• Tier two, **mission/business process level --** designing, developing, and implementing the missions and business processes that support the missions and business functions defined at Tier 1; and

• Tier three, **information system level --** integrating risk management activities into the system development life cycle of information systems from the initiation of a system, through development, implementation, operation, maintenance, and disposal.

At Tiers 1 and 2, organizations can use risk assessments to evaluate systemic information security-related risks that are associated with organizational governance and management activities, missions and business processes, enterprise architecture, or the funding of information security programs.

At Tier 3, organizations can use risk assessments to more effectively support the implementation of the **Risk Management Framework (RMF)**, which provides for:

- Categorizing the information system and its information based on the potential adverse impacts to the organization;
- Selecting, implementing, and assessing an appropriate set of security controls for the information system and the environment in which the system operates;

- Authorizing the information system operation based upon a determination of the risk and a decision that the risk is acceptable; and
- Monitoring and assessing selected security controls in the information system on a continuous basis, documenting changes to the system, conducting security impact analyses of the changes, and reporting the security status of the system to organizational officials.

Conducting Risk Assessments

Risk assessments are conducted on an ongoing basis to provide important information for organizational decision makers to help guide and inform their responses to information security risks. Organizations can apply risk assessments throughout the system development life cycle and across all of the tiers in the risk management hierarchy, based on management decisions about the frequency of conducting such assessments and the resources to be applied.

Continuing communications and information sharing among organizational participants in the risk assessment process help to ensure that the inputs to assessments are accurate, that intermediate results can be used across the organizational tiers, and that the results are meaningful and useful inputs to the risk response step in the risk management process.

The risk assessment process consists of four steps:

• **Preparing** for the assessment. This step establishes a context for the risk assessment by applying the results from the risk framing step of the risk management process. Risk framing identifies organizational information regarding policies and requirements for conducting risk assessments, specific assessment methodologies to be employed, procedures for selecting risk factors to be considered, scope of the assessments, rigor of analyses, degree of formality, and requirements that facilitate consistent and repeatable risk determinations across the organization. Organizations should use the risk management strategy to the extent practicable to obtain the needed information for the risk assessment and to prepare for the assessment.

• **Conducting** the assessment. This step produces a list of information security risks that can be prioritized by risk level and used to inform risk response decisions. Organizations analyze threats and vulnerabilities, impacts and likelihood of harm, and the uncertainty associated with the risk assessment process. They also gather essential information as a part of each task to assure that this step is conducted in accordance with the assessment context established in the previous step. The objective is to adequately cover the entire threat environment in accordance with the specific definitions, guidance, and direction established during the first step. To

achieve adequate coverage within available resources, organizations may have to generalize threat sources, threat events, and vulnerabilities, and to assess specific, detailed sources, events, and vulnerabilities as necessary to accomplish risk assessment objectives.

• **Communicating** assessment results. This step communicates the assessment results and promotes the sharing of risk-related information. This step helps to ensure that decision makers across the organization have the appropriate risk-related information needed to inform and guide their risk decisions. Information to be communicated and shared includes the risk assessment results and the information that is developed in the risk assessment process.

• **Maintaining** the assessment. In carrying out this step, organizations should maintain the currency of their specific knowledge of the risk situation. The results of risk assessments inform risk management decisions and guide risk responses. To support the ongoing review of risk management decisions, organizations should maintain their risk assessments by incorporating any changes detected through risk monitoring. Risk monitoring provides organizations with an ongoing capability to determine the effectiveness of risk responses, to identify risk-impacting changes to organizational information systems and their operating environments, and to verify compliance.

SP 800-30 Revision 1 divides each step of the risk assessment process into a set of tasks, and provides detailed guidance for each task. Supplemental guidance and additional information for organizations conducting risk assessments are included in the supporting appendices to the publication.

For More Information

The risk assessment approach described in SP 800-30 Revision 1 is supported by other security standards and guidelines that have been issued for managing information security risk. The publications listed below were developed by the Joint Task Force to advance the unified information security framework for the federal government.
These publications are available here.

Each of these publications was the subject of an ITL Bulletin summarizing the contents of the publication. The bulletins are available below.

• NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
ITL Bulletin

NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
ITL Bulletin

• NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*
ITL Bulletin

• NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*
ITL Bulletin

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) publish standards for risk management and information security including:

• ISO/IEC 31000, *Risk management – Principles and guidelines*;

• ISO/IEC 31010, *Risk management – Risk assessment techniques*;

• ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements*; and

• ISO/IEC 27005, *Information technology – Security techniques – Information security risk management systems*.

NIST works with public and private sector organizations to establish relationships between NIST standards and guidelines and the standards developed by ISO and IEC. The practices recommended in SP 800-30 Revision 1 are consistent with the concepts and principles expressed in these international standards, which are available here.

General information about the Risk Management Framework, and access to standards and guidelines that pertain to the RMF, are available here.

The FISMA Implementation Project leader and the NIST contact for more information about risk management activities is:

Dr. Ron Ross
301-975-5390
Email ron.ross@nist.gov

Information about NIST's information security programs is available from the Computer Security Resource Center here.

ITL Bulletin Publisher:
Elizabeth Lennon, Writer/Editor
Information Technology Laboratory
National Institute of Standards and Technology
Email elizabeth.lennon@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.