ITL BULLETIN FOR MARCH 2011

MANAGING INFORMATION SECURITY RISK: ORGANIZATION, MISSION AND INFORMATION SYSTEM VIEW

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

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. All of these activities have an impact on the success of the organization in carrying out its mission and business processes. Organizations can effectively manage the risk associated with these activities by adopting an integrated approach, bringing 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 is an essential element of the organization's overall risk management process. Many organizations operate in highly complex, interconnected environments using state-of-the-art and legacy information systems, and they depend on information systems to carry out their mission and business functions. Well-informed risk-based decisions enable organizations to balance the benefits gained from the operation and use of information systems with the risk of operational disruptions, human and system errors, and hostile attacks. Because of the reliance on information systems, the effective management of information security risk is critical to the success of an organization in achieving its strategic goals and objectives.

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) recently issued a new guide to assist organizations in managing the risk associated with the operation and use of information systems within the broad context of achieving organizational mission and business goals. The new publication introduces an integrated approach to organization-wide risk management that links risk-based decisions affecting information security with the risk-based decisions affecting all aspects of the organization's important mission and business functions.

NIST Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission and Information System View*

NIST Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission and Information System View,* is the fourth in the series of risk management and information security guidelines that are being developed by the Joint Task Force, a joint 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.

The Federal Information Security Management Act (FISMA) of 2002 directs federal agencies to develop, document, and implement programs to protect their information and information systems, and requires that agencies 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.

NIST SP 800-39 provides a structured, yet flexible approach for managing risk that is supported by other NIST security standards and guidelines. See the Other Publications section below for a link to NIST security standards and guidelines. The new publication discusses the basic concepts of risk management as 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.

The guide introduces a three-tiered risk management approach that allows organizations to establish an enterprise-wide risk management strategy as part of a mature governance structure, involving senior leaders and executives, and including a risk executive (function). The three-tiered approach addresses risk at:

• The **organization level**;
• The **mission/business process level**; and
• The **information system level**.

The four components of the risk management process are discussed in connection with their applicability across the three tiers of risk management. This approach enables organizations to integrate the risk management process throughout the organization.

The life cycle-based process for managing information security risk is described in the guide, with details provided for each component of the risk management process and with consideration given to changing mission and business needs, operating environments, and supporting information systems. Each step in the process is described with a focus on the inputs or preconditions necessary to initiate the step, the specific activities that compose the step, and the outputs or post conditions resulting from the step. Also discussed are risk concepts, including risk tolerance, trust, and organizational culture, in the context of the risk management process and its multitiered application.

Supporting appendices provide additional risk management information including general references, definitions and terms, and acronyms. One part of the appendices discusses the roles and responsibilities of the key participants involved in the risk management process. A chart summarizes the specific tasks for the components in the risk management process. Other information in the appendices includes centralized, decentralized, and hybrid approaches to the governance of information security and risk management; model ways that organizations can obtain the levels of trust needed to form partnerships, collaborate with other organizations, share information, or receive information system and security services; and strategies for responding to each type of risk.

NIST SP 800-39, *Managing Information Security Risk: Organization, Mission and Information System View*, is available at the NIST Web page http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

Components of Risk Management Activities

Managing risk is a complex, multifaceted activity involving people throughout the entire organization from senior and mid-level leaders to the individuals who operate the information systems.

The first component in the risk management process requires organizations to **frame risk,** or establish a context in which risk-based decisions are made. This activity produces a risk management strategy that addresses the next three components in the process: how the organization intends to assess risk, respond to risk and monitor risk.

The risk frame establishes a foundation for managing risk and delineates the boundaries for risk-based decisions within the organization. To establish a risk frame, the organization must identify its assumptions about risk, including the threats, vulnerabilities, consequences, impact, and likelihood of occurrence of harm to the organization. These assumptions affect how risk is assessed, responded to, and monitored over time. The organization also identifies constraints on the risk assessment, response, and monitoring alternatives under consideration, its risk tolerance, and its priorities and trade-offs. The risk framing component and the associated risk management strategy also include any strategic-level decisions on how risk to organizational operations and assets, individuals, other organizations, and the Nation, is to be managed by senior leaders and executives.

The second component of risk management concerns how organizations **assess risk** within the context of the organizational risk frame. The organization identifies threats to its operations, assets, or individuals, or threats directed to other organizations. Other issues addressed include vulnerabilities internal and external to organizations; the harm that might occur if the threats exploit known vulnerabilities; and the likelihood that harm will occur. The result of this assessment is a determination of risk, both the degree of harm and likelihood of harm occurring.

The third component of risk management involves how organizations **respond to risk** once that risk is determined based on the results of risk assessments. The risk response component provides a consistent, organization-wide response to risk in accordance with the organizational risk frame by developing and evaluating alternative courses of action, and by determining and implementing appropriate courses of action. Organizations describe the types of risk responses that can be implemented: accepting, avoiding, mitigating, sharing, or transferring risk. They also identify the tools, techniques, and methodologies used to develop courses of action for responding to risk, how courses of action are evaluated, and how risk responses are communicated both internally and externally.

The fourth component of risk management deals with how organizations **monitor risk** over time. This involves describing how compliance to information security requirements is verified and how the ongoing effectiveness of risk responses is determined, including the tools, techniques, and methodologies used to determine the sufficiency and correctness of risk responses and the correct implementation of risk mitigation measures. In addition, organizations describe how changes that may impact the ongoing effectiveness of risk responses are monitored.

Multitiered Risk Management

The risk management process is integrated throughout the organization through a three-tiered approach to achieve continuous improvement in risk-related activities and to facilitate effective communication throughout the organization.

Tier 1, organizational level, addresses 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, and missions and business functions. Governance structures provide oversight for the risk management activities conducted by organizations and include the establishment and implementation of a risk executive (function); the establishment of the organization's risk management strategy including the determination of risk tolerance; and the development and execution of organization-wide investment strategies for information resources and information security.

Tier 2, mission/business process level, encompasses designing, developing, and implementing mission/business processes that support the functions defined at Tier 1. Organizational mission/business processes guide and inform the development of an enterprise architecture that provides a disciplined and structured methodology for managing the complexity of the organization's information technology infrastructure. The enterprise architecture includes an embedded information security architecture, which is structured to ensure that the information security requirements and protection needs of this process level are defined and allocated to appropriate organizational information systems and to the environments in which those systems operate.

Tier 3, information system level, integrates risk management activities into the system development life cycle of organizational information systems, from the initiation of a system, through development, implementation, operation, maintenance, and disposal. These risk management activities reflect the organization's risk management strategy and any risk related to the cost, schedule, and performance requirements for individual information systems supporting the mission/business functions of organizations. Risk management activities take place at every phase in the system development life cycle with the outputs at each phase having an effect on subsequent phases. All information systems, including operational systems, systems under development, and systems undergoing modification, are in some phase of the system development life cycle.

The risk management process applied across the three tiers of an organization is illustrated in the figure below.

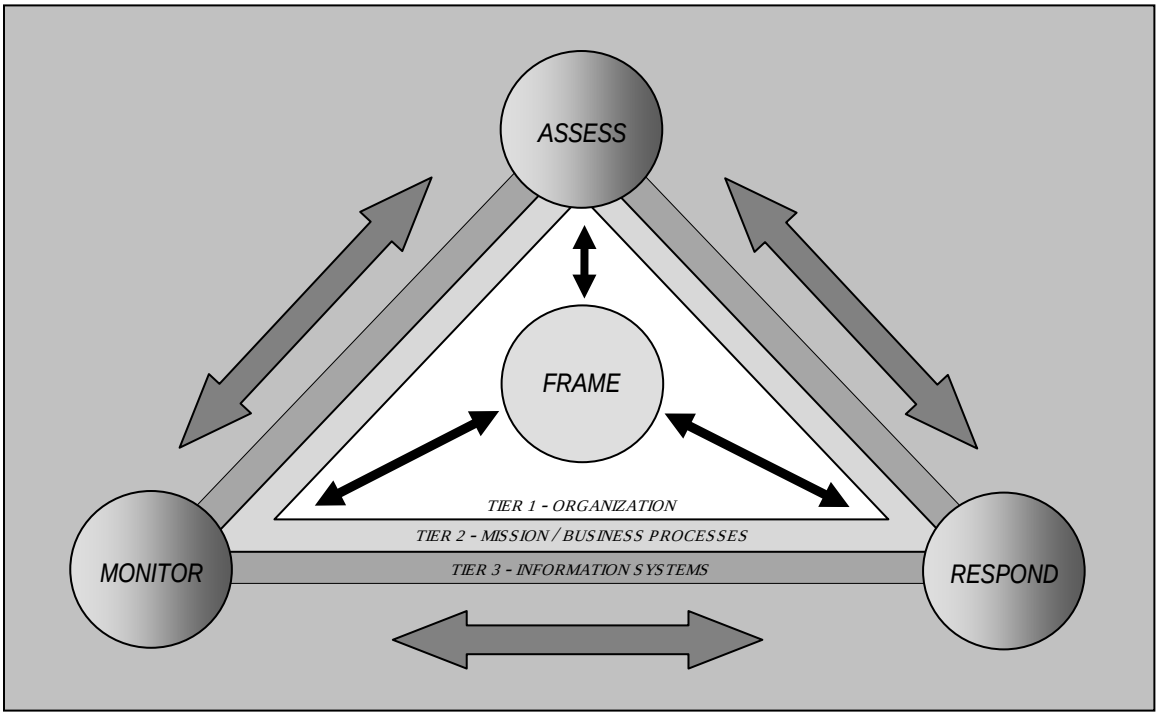

FIGURE: RISK MANAGEMENT PROCESS APPLIED ACROSS THE TIERS

The multitiered risk management approach ensures that strategic considerations, including top-level organizational goals and objectives, drive investment and operational decisions with regard to managing risk to the organization, other organizations, and the Nation. This type of risk-based decision making is especially important in dealing with advanced persistent threats and potential attacks that can degrade or debilitate federal information systems supporting the critical applications and operations of the federal government.

Risk-related concepts also must be considered in the risk management process. These include risk tolerance, the levels of risk, types of risk, and degree of risk uncertainty that

are acceptable; trust, the belief that an entity will behave in a predictable manner in specified circumstances; and organizational culture, the values, beliefs, and norms that influence the behaviors and actions of the senior leaders, executives, and individual members of organizations. These risk-related concepts can have an impact on risk management, and the concepts may interact with each other in ways that influence the pace of change and the implementation of the risk management strategy.

Other Publications

The risk management approach described in NIST SP 800-39 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 at the NIST Web page http://csrc.nist.gov/publications/PubsSPs.html.

Each of these publications was the subject of an *ITL Bulletin* summarizing the contents of the publication. The bulletins are available at the Web page indicated:

• SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
Bulletin: http://csrc.nist.gov/publications/nistbul/march2010_sp800-37rev1.pdf

• SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*
Bulletin: http://csrc.nist.gov/publications/nistbul/Aug2009_sp800-53-rev3_bulletin.pdf

• SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*
Bulletin: http://csrc.nist.gov/publications/nistbul/august2010-bulletin.pdf

NIST SP 800-39 supersedes NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, as the source for guidance on risk management. NIST and the Joint Task Force are developing a revised NIST SP 800-30, *Guide for Conducting Risk Assessments*, which is expected to be issued in 2011, and which will be a companion document to NIST SP 800-39.

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 private and public sector organizations to establish relationships between NIST standards and guidelines and the standards developed by ISO and IEC. The practices recommended in NIST SP 800-39 are consistent with the concepts and principles expressed in these international standards, which are available at http://www.iso.org/iso/store.htm.

For More Information

General information about the Risk Management Framework (RMF), and access to standards and guidelines that pertain to the RMF, are available from the NIST Web page http://csrc.nist.gov/groups/SMA/fisma/framework.html.

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

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

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.