February 2002

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

RISK MANAGEMENT GUIDANCE FOR INFORMATION TECHNOLOGY SYSTEMS

By Joan S. Hash, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology

This ITL Bulletin describes risk management methodology and how to integrate it into an information technology (IT) security program. This means effectively integrating it into an organization's systems development life cycle (SDLC). Key to implementation of a successful enterprise-wide IT security program is the ability to identify and protect critical information assets. A sound risk management program is the enabler needed to make the implementation successful. The bulletin summarizes NIST Special Publication 800-30*, Risk Management Guide For Information Technology Systems*, by Gary Stoneburner, Alice Goguen, and Alexis Feringa, which is available for download at http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

The ability to address current concerns regarding threats against the nation's critical infrastructures, cost-effective security, and continuity of operations all depend upon the use of effective risk management processes which support sound *risk-based decision-making*. Risk management is an essential management function and should not be treated solely as a technical function relegated to IT operational or security personnel for implementation. Organizational management charged with overall responsibility for IT infrastructures (i.e., Chief Information Officers [CIOs], agency heads) needs to define and ensure implementation of an effective and comprehensive risk management program, which encompasses all segments of the enterprise and supports the organizational mission.

Risk Management Overview

Risk is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. The objective of performing risk management is to enable the organization to accomplish its mission(s) (1) by better securing the IT systems that store, process, or transmit organizational information; (2) by enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget; and (3) by assisting management in authorizing (or accrediting) their IT systems on the basis of the supporting documentation resulting from the performance of risk management.

Risk management encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment. Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions. This process is not unique to the IT environment; indeed it pervades decision-making in all areas of our daily lives. Take the case of home security, for example. Many people decide to have home security systems installed and pay a monthly fee to a service provider to have these systems monitored for the better protection of their property. Presumably, the homeowners have weighed the cost of system installation and monitoring against the value of their household goods and their family's safety, a fundamental "mission" need.

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 August 2000

Integrating Risk Management Into The System Development Life Cycle (SDLC)

Risk management is an iterative process and has activities relevant to every phase of the life cycle. Minimizing negative impact on an organization and the need for a sound basis in decision-making are the fundamental reasons that organizations implement a risk management process for their IT systems. An IT system's SDLC has five phases: initiation, development or acquisition, implementation, operation or maintenance, and disposal. The chart below summarizes risk management activity associated with each phase of the SDLC.

The Risk Assessment Methodology

Risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an IT system throughout its SDLC. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process. ***Risk*** is a function of the ***likelihood*** of a given ***threat-source*** exercising a particular potential ***vulnerability*** and the resulting ***impact*** of that adverse event on the organization.

To determine the likelihood of a future adverse event, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT system. Impact refers to the magnitude of harm that could be caused by a threat's exercise of a vulnerability. The level of impact is governed by the potential mission impacts and in turn produces a relative value for the IT assets and resources affected (e.g., the criticality and sensitivity of the IT system components and data). The risk assessment methodology encompasses nine primary steps.

- **Step 1—System Characterization:** The first step is to define the scope and activities of interest including all system boundaries, information and resources, which constitute the domain of interest. This includes as a minimum hardware and software, internal and external system interfaces, data and information used or produced by the system, system support personnel activities, user interfaces and processes performed, system and data criticality, and system and data sensitivity.
- **Step 2—Threat Identification:** A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. A vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present a risk when there is no vulnerability that can be exercised. In determining the likelihood of a threat, one must consider threat-sources, potential vulnerabilities, and existing controls. The goal of this step is to identify potential threat-sources and compile a threat statement listing potential threat-sources that are applicable to the IT system being evaluated.
- **Step 3—Vulnerability Identification:** The analysis of the threat to an IT system must include an analysis of the vulnerabilities associated with the system environment. The goal of this step is to develop a list of system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources. The

SDLC Phases	Phase Characteristics	Support from Risk Management Activities
Phase 1—Initiation	The need for an IT system is expressed, and the purpose and scope of the IT system are documented.	• Identified risks are used to support the development of the system requirements, including security requirements and a security concept of operations (strategy).
Phase 2—Development or Acquisition	The IT system is designed, purchased, programmed, developed, or otherwise constructed.	• The risks identified during this phase can be used to support the security analyses of the IT system that may lead to architecture and design trade-offs during system development.
Phase 3—Implementation	The system security features should be configured, enabled, tested, and verified.	• The risk management process supports the assessment of the system implementation against its requirements and within its modeled operational environment. Decisions regarding risks identified must be made prior to system operation.
Phase 4—Operation or Maintenance	The system performs its functions. Typically the system is being modified on an ongoing basis through the addition of hardware and software and by changes to organizational processes, policies, and procedures.	• Risk management activities are performed for periodic system reauthorization (or reaccreditation) or whenever major changes are made to an IT system in its operational, production environment (e.g., new system interfaces).
Phase 5—Disposal	This phase may involve the disposition of information, hardware, and software. Activities may include moving, archiving, discarding, or destroying information and sanitizing the hardware and software.	• Risk management activities are performed for system components that will be disposed of or replaced to ensure that the hardware and software are properly disposed of, that residual data is appropriately handled, and that system migration is conducted in a secure and systematic manner.

table at right gives examples of vulnerability/threat pairs.

- **Step 4—Control Analysis:** The goal of this step is to analyze the controls that have been implemented or planned for implementation by the organization to minimize or eliminate the likelihood (or probability) of a threat's exercising a system vulnerability. To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the implementation of current or planned controls must be considered.
- **Step 5—Likelihood Determination:** To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the following governing factors must be considered: ***Threat-source motivation and capability, nature of the vulnerability, and existence and effectiveness of current controls.***
- **Step 6—Impact Analysis:** The next major step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of a vulnerability. The adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any, of the following three security goals: ***integrity, availability, and confidentiality***.
- **Step 7—Risk Determination:** The purpose of this step is to assess the level of risk to the IT system. The determination of risk for a particular threat/vulnerability pair can be expressed as a function of:
  *The **likelihood** of a given threat-source's attempting to exercise a given vulnerability*
  *The **magnitude of the impact** should a threat-source successfully exercise the vulnerability*
  *The **adequacy of** planned or existing security **controls** for reducing or eliminating risk.*
- **Step 8—Control Recommendations:** During this step of the process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization's operations, are provided. The goal of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks: ***Effectiveness of recommended options (e.g., system compatibility), Legislation and regulation, Organizational policy, Operational impact, Safety and reliability.***
- **Step 9—Results Documentation:** Once the risk assessment has been completed (threat-sources and vulnerabilities identified, risks assessed, and recommended controls provided), the results should be documented in an official report or briefing. A risk assessment report is a management report that helps senior management, the mission owners, make decisions on policy, procedural, budget, and system operational and management changes. Unlike an audit or investigation report, which looks for wrongdoing, a risk assessment report should not be presented in an accusatory manner but as a systematic and analytical approach to assessing risk so that senior management will understand the risks and allocate resources to reduce and correct potential losses.

Vulnerability	Threat-Source	Threat Action
Terminated employees' system identifiers (IDs) are not removed from the system.	Terminated employees	Dialing into the company's network and accessing company proprietary data
Company firewall allows inbound telnet, and *guest* ID is enabled on XYZ server.	Unauthorized users (e.g., hackers, terminated employees, computer criminals, terrorists)	Using telnet to XYZ server and browsing system files with the *guest* ID
The vendor has identified flaws in the security design of the system; however, new patches have not been applied to the system.	Unauthorized users (e.g., hackers, disgruntled employees, computer criminals, terrorists)	Obtaining unauthorized access to sensitive system files based on known system vulnerabilities

Risk Mitigation

Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process. Because the elimination of all risk is usually impractical or close to impossible, it is the responsibility of senior management and functional and business managers to implement the ***most appropriate controls*** to decrease mission risk to an acceptable level, with ***minimal adverse impact*** on the organization's resources and mission ***(cost-effective risk management).*** Risk mitigation is a systematic methodology used by senior management to reduce mission risk. Risk mitigation can be achieved through any of the following risk mitigation options:

- **Risk Assumption.** To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level
- **Risk Avoidance.** To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified)
- **Risk Limitation.** To limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls)
- **Risk Planning.** To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls
- **Research and Acknowledgment.** To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability
- **Risk Transference.** To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

Cost-Benefit Analysis and Residual Risk

A cost-benefit analysis for proposed new controls or enhanced controls encompasses the following:

- Determining the impact of implementing the new or enhanced controls
- Determining the impact of not implementing the new or enhanced controls
- Estimating the costs of the implementation. These may include, but are not limited to, the following: *Hardware and software purchases, Reduced operational effectiveness if system performance or functionality is reduced for increased security, Cost of implementing additional policies and procedures, Cost of hiring additional personnel to implement proposed policies, procedures, or services, Training costs, Maintenance costs.*
- Assessing the implementation costs and benefits against system and data criticality to determine the importance of implementing the new controls, given their costs and relative impact.

Organizations can analyze the extent of the risk reduction generated by the new or enhanced controls in terms of the reduced threat likelihood or impact, the two parameters that define the mitigated level of risk to the organizational mission. ***The risk remaining after the implementation of new or enhanced controls is the residual risk.*** Practically no IT system is risk free, and not all implemented controls can eliminate the risk they are intended to address or reduce the risk level to zero. If the residual risk has not been reduced to an acceptable level, the risk management cycle must be repeated to identify a way of lowering the residual risk to an acceptable level. Once the management official responsible for the IT infrastructure determines that an acceptable level of risk has been achieved, the official should sign a statement indicating acceptance of the residual risk prior to authorization or accreditation of the system for full operation.

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.

Keys To Successful Risk Management

A successful risk management program will rely on (1) senior management's commitment for necessary resources and time; (2) the full support and participation of the IT team; (3) the competence of the risk assessment team, which must have the expertise to apply the risk assessment methodology to a specific site and system, identify mission risks, and provide cost-effective safeguards that meet the needs of the organization; (4) the awareness and cooperation of members of the user community, who must follow procedures and comply with the implemented controls to safeguard the mission of their organization; and (5) an ongoing evaluation and assessment of the IT-related mission risks. Although OMB Circular A-130 mandates a risk management process, risk management should be conducted and integrated into the SDLC not because it is required by directive but because it is good practice in support of the overall mission.

Ten Most Frequently Asked Questions On Risk Assessment

1. ***What is the difference between a qualitative and quantitative risk assessment?***
   A quantitative risk assessment expresses threat likelihood (probability), impact, and risk in terms of a numeric value, whereas a qualitative assessment uses ratings of *high, medium, or low* to express the value. The major advantage of the quantitative approach is that it provides a measurement, which can be fed directly into a cost-benefit analysis. However, unless the metrics used are comprehensive, consistent, accurate and relevant, this approach has little or no benefit over a qualitative approach since some subjective interpretation must still be applied. Many approaches today start by using the qualitative rankings (*high, medium, or low*) and attribute a range of values to each.
2. ***Who should participate in a risk assessment exercise?***
   For the subject system(s), the team should include as a minimum the following representatives: *system owner(s), IT security representative, operational system users, and IT system support personnel. Others may be added to the team, as management deems appropriate.*
3. ***How long should a risk assessment take?***
   The length of time required to complete a risk assessment varies based on the scope and complexity of the subject system as well as the commitment in amount and skill level of resources assigned.

Who we are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our web site is http://www.itl.nist.gov/.

Typically, risk assessments of average, non-complex application systems can be completed in three months or less. More complex support systems (*networks, data centers)* or applications may require six to nine months on average. When all or part of the risk assessment is outsourced, the timeline is dependent upon availability and expertise of contract resources.

4. ***How often should risk assessments be conducted?***
Every system under development should be subjected to a risk assessment as part of the SDLC and prior to certification and accreditation. Systems in operational status should be subjected to a risk assessment whenever there is a major change in functionality or IT architecture. OMB Circular A-130 requires that application and support systems undergo a risk assessment at least once every three years. In addition, the Government Information Security Reform Act (GISRA) of 2000 requires agencies to conduct annual reviews of their security programs including system testing. Clearly, agencies may decide to do different degrees of testing for different systems (e.g., more testing for mission-critical systems).

5. ***Who should receive the final risk assessment report?***
The final report should be submitted to the responsible System owner who should use it to make decisions regarding system readiness. The manager will either determine that more controls are warranted prior to system approval or that the degree of risk is acceptable. Since risk assessment documents are subject to the "need to know" principle, management should direct further distribution of the documents.

6. ***How do I derive a risk determination?***
Determination of risk is derived as follows:

Threat likelyhood (probability) **X** ***Threat Impact*** **=** ***Derived Risk***

(*For an example, refer to NIST Special Publication 800-30.)*

7. ***How does one attribute costs to "intangible" impacts?***
It is difficult to put a cost figure on intangibles such as reputation and public trust. However, case studies of impact on business and customer base due to system weaknesses or loss of confidence, customer surveys used to assess potential impact, and use of focus groups are methods which can be applied to try to address intangibles.

8. ***How do I capture threat source information?***
Threat information is available from sources such as state and local entities tracking natural and environmental threats (i.e., weather service) as well as local utilities. In addition, human threat source information is available from federal and local law enforcement sources. Government agencies also receive information from their Office of Inspectors General (OIG), National Infrastructure Protection Center (NIPC), FedCIRC, and other computer emergency response services. The mass media is also an excellent source of information. In addition, the Internet provides a great resource for research in this area. Most risk assessment vendors have robust databases on threats as well.

9. ***What are good sources of vulnerability information?***
Results from prior audits, previous risk assessment reports, General Accounting Office (GAO) reports, OIG reports, fraud reports, error and exception reports produced by the system, security requirements documentation, and industry white papers and other publications are all good sources. A key resource available at NIST is the ICAT tool, which can be found at http://icat.nist.gov. This tool provides an index to identified system vulnerabilities and information on patches available to correct the vulnerability.

10. ***How should this methodology be applied for multiple interacting systems****?*
Each system involved in the interaction should have gone through a risk assessment first. After that has been completed, the scope of the interaction must be defined in terms of system interfaces, user interfaces, connectivity, data/information flow, and additional functionality to be implemented as a result of the interaction. The steps applied are the same but the complexity and depth of the analysis is dependent upon the nature of the interaction and defined domain of interest. The effort required to do this when the interaction is less than trivial may be rather extensive.

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