

realtimepublishers.comtm

The Practical Guidetm To

Managing Risks



Rebecca Herold

The Practical Guide to Managing Risks	1
Who Are Your Stakeholders?	2
What Are Your Value Drivers?	4
Managing Risks Throughout the Organization.....	4
Defining Vulnerability and Threat.....	5
Defining Risk	8
Cost-Benefit Analysis	8
Identifying Assets at Risk.....	9
Identifying Asset Values and Impacts	9
Residual Risk	10
What Is an Information Security Event?.....	11
Determining Probability of an Event	12
Considering the Impacts of an Event	12
Considering Likelihood and Impact.....	13
Common Risk Reduction Models.....	14
Basel II.....	14
COSO.....	14
ISO Guide 73	15
NIST Special Publication 800-30	15
Prioritizing Risks	15
Be Strategic When Managing Risk.....	16
Building a Risk Management Roadmap	17
Integrating Information Security Risk Management into the Enterprise.....	18
Using Qualitative and Quantitative Measures	18
Identifying Business Drivers.....	18
Identifying Risk Drivers	19
Establishing Metrics.....	19
Providing Training	19
Providing Continuous Communication.....	19
Using Appropriate Tools.....	19
Integrating Risk Management Into The System Development Life Cycle.....	19
Phase 1: Project Initiation	20
Phase 2: Development or Acquisition.....	20

Phase 3: Implementation.....	20
Phase 4: Operation or Maintenance	20
Phase 5: Disposal	20
The Information Security Risk Management Methodology	21
Step 1: System Characterization	21
Step 2: Threat Identification	21
Step 3: Vulnerability Identification	21
Step 4: Control Analysis	21
Step 5: Likelihood Determination.....	22
Step 6: Impact Analysis	22
Step 7: Risk Determination.....	22
Step 8: Control Recommendations	22
Step 9: Results Documentation.....	23
Mitigating Risk	23
Information Security Risk Management Strategy.....	24
Step 1: Identify Events.....	25
Step 2: Identify Assets	25
Step 3: Identify Threats.....	25
Step 4: Identify Impacts	25
Step 5: Produce Risk Reduction Plans.....	25
Step 6—Follow Up and Verify that Actions Have Occurred	26
Summary	26

Copyright Statement

© 2004 Realtimedpublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimedpublishers.com, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimedpublishers.com, Inc or its web site sponsors. In no event shall Realtimedpublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimedpublishers.com and the Realtimedpublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimedpublishers.com, please contact us via e-mail at info@realtimedpublishers.com.

The Practical Guide to Managing Risks

Every organization has a mission. Most, if not all, organizations use information technology (IT) to process their information in support of their missions and reaching their business goals. Managing risks associated with the information and supporting technologies is a critical factor in successful organizational mission realization.

The primary goal of an organizational risk management program should be to protect the organization and its ability to achieve its mission. Protecting the information and IT assets are a component of this program, but IT professionals must always remember the business components. Risk management should not be handled primarily as a technical function carried out by the IT experts who operate and manage the IT system, but instead risk management must be considered as an essential management function of the business.

Executive management must visibly and actively support the IT security risk management component of the complete business risk management process. This sponsorship is vital to ensure that stakeholders do not resist or undermine efforts to use risk management to make the organization more secure and protect the health of the organization. Without this clear executive sponsorship, personnel tend to disregard the directives, policies, and procedures for how to perform their job responsibilities and duties in a secure manner to protect information and technology assets. Executive sponsors should demonstrate their support of the risk management program by:

- Delegating authority and responsibility for a clearly defined risk management project scope to one area of the company, such as the IT risk management team or a Chief Risk Officer.
- Supporting, or better yet mandating, participation by all personnel as appropriate and needed to successfully fulfill the program.
- Allocating sufficient resources, such as personnel and financial backing.
- Issuing communications that clearly and actively support the risk management process, identifying specifically the IT security risk management components so that they are viewed as part of the entire enterprise risk management process.
- Participating in reviewing the findings and recommendations of the security risk management process and supporting the program's recommendations.



An effective risk management program helps an organization meet business objectives by ensuring that resources are allocated to plan, make decisions, and carry out activities. Unlike other business management activities, risk management focuses on the uncertainties that organizations face; uncertainties in the probability of the occurrence of events, uncertainties in the value of the consequences of the events to the organization, and so on.

Highly publicized incidents, such as the Enron collapse and the Tyco tax evasion investigation, have resulted in making risk management a requisite management activity within all business enterprises. Managing risk through the use of effective risk management frameworks will ensure efficiency and comprehensive risk consideration. Effective risk management frameworks describe an organization's specific set of functional business activities and associated definitions that specify the processes that will be used to manage risks. An effective risk management framework will enhance and improve business risk management, including IT security risk management, by

- Making risk management more transparent and understandable to stakeholders.
- Making risk management processes more efficient.
- Allowing for sharing of best practices in the implementation of risk identification, risk assessment, and risk treatment.
- Showing executives that the process is well thought out; providing for a better chance of obtaining strong executive support.

Who Are Your Stakeholders?

The first step in addressing the organization's information security risks is to identify the key business stakeholders. Stakeholders can be any person, group, or entity that can place a claim on the organization's attention, resources, or output or that is affected by that output. Stakeholders in a corporation are those persons or entities that bear some form of risk as a result of having invested some type of capital—human or financial—that is placed at risk as a result of the organization's activities or have regulatory authority over that organization. Stakeholders may be internal or external.


Once stakeholders have been identified, list the interests, benefits, and outputs that these stakeholders demand from your organization, such as:

- Shareholder value
- Compliance with regulations
- Product safety
- Privacy of personal information

Stakeholders can place a claim on the organization's resources and, so, are themselves a source of risk. Possible stakeholders include:

- Employees
- Suppliers and business partners
- Governmental entities
- Regulators
- Shareholders
- Rating agencies
- Customers
- Management/Board of Directors
- Surrounding communities

Stakeholders drive decision-making within organizations and influence performance. Their requirements and concerns will shape and focus your information security risk program. An effective risk management program that fully addresses key stakeholders can free executive time, allowing them to focus on activities that will create new value for stakeholders.

 Understand the inputs to and outputs from the organization. Anyone that has an investment in the organization can be considered a stakeholder, whether the investment is in the form of financial, human, or knowledge capital. Suppliers would also typically be considered a stakeholder. Everyone impacted or potentially impacted by an output can also be considered a stakeholder.

Positions within the company that are responsible for risk management—such as, facilities security and risk, audit, and other control functions—are considered key stakeholders and have a direct impact on the information security risk management program. It is important to define the roles and responsibilities of the various risk management functions, including:

- Managing decisions, activities, and processes
- Approving key decisions
- Providing input for decisions, activities, and processes
- Receiving information about outcomes related to various decisions, activities, and processes

What Are Your Value Drivers?

As defined by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission within their Enterprise Risk Management (ERM) framework, a value driver is “a measure of the strategies, processes, activities, or assets that create value and whether they are being utilized in a manner that creates sustainable value.” Typical stakeholder value drivers include increasing revenue growth, lowering the cost structure of the business, and ensuring the continuity of operations.

☞ To be successful, information security risk managers must understand what creates value and how that value can be improved. Business value, not just IT-specific value, must be considered.

Identify potential value drivers for each key stakeholder group. Limit the value drivers to those that your information security risk management program can impact in a significant way. Determine how you will describe and group potential impacts and the organization’s decisions to accept those impacts.

Managing Risks Throughout the Organization

The objective of managing organization risk is carried out by a specified set of processes defined in a risk management framework. The objective is supported by the organization’s risk management system and defined within roles and responsibilities.

☞ Risk management should be a line management function not a staff function. It is a management activity and is integral with decision-making. As Peter Drucker, celebrated “father of modern management” puts it, “a decision that does not involve risk, probably is not a decision.”

Organizations must direct and manage IT activities to reach an effective balance between managing risks and realizing business benefits. All business activities are performed under some degree of risk. Effective business management that incorporates information security risk management will help to avert threats and reduce potential harm to the organization.

Effective information security risk management is only sustainable in an organization if there is constant attention paid to addressing risks in the form of audits, reviews, and other forms of monitoring. Because of the perceived low probability nature of most risks relative to other management tasks, they are often put on the back burner and their predominantly negative characteristics make it easier to decide to address them on another day. Unless the organization is vigilant, risk management controls quickly become ineffective.

Each organization must design its own risk management framework, process, roles and responsibilities, documentation, and so on. However, there are standard risk management functional elements for the framework and procedures that should be used in the design. These elements will ensure that the risk management procedures will be understood and supported by others and will improve both effectiveness and efficiency. Key indicators of effective risk management activity in an organization are:

- Visible support and commitment of senior management
- Risk controls and programs that are ubiquitous in the organization and well understood
- A documented risk profile that establishes priorities for modifying risk controls
- Effective risk communication for employees and other stakeholders
- Monitor and review of performance indicators of the organization's risks
- Knowledge and documentation of all legal and regulatory requirements
- An ongoing, repeatable process that is integrated into the organization's culture

Information security risk management must produce a net value for the organization. This value is estimated using three basic elements: costs, financial benefits, and trust and respect of stakeholders and the public.

Defining Vulnerability and Threat

Vulnerabilities are weaknesses associated with organizational assets. Vulnerability is a condition or set of conditions that may allow a malicious or accidental threat to affect an asset, either with greater frequency, greater impact, or both. A vulnerability that cannot be exploited by a threat is not harmful to the asset. Vulnerability is a characteristic of an information asset or group of information assets that can be exploited by a threat.

Vulnerability is often a consequence of a poor management decision, flawed procedures, under-skilled staff, incorrectly configured systems, defective technology, and so on. For a vulnerability to be exploitable, it must be known to or discoverable by a threat. Thus, it is important to monitor access control regarding information security and apply it to both people and technology.



Vulnerability is a characteristic of a system, asset or an organization, in contrast to a threat, which originates from either inside or outside the system, asset, or organization.

Examples of Information Vulnerabilities

The following list highlights examples of information vulnerabilities. The list has been divided into categories for readability.

Physical Vulnerabilities

- Availability of flammable materials such as paper or boxes
- Improper or inappropriate cabling or maintenance of technical facilities
- Inadequate monitoring of environmental conditions
- Lack of automatic fire suppression system, back-up facilities or processes, environmental protection, fire detection devices, maintenance of equipment and facilities, power conditioning equipment, or uninterruptible power supply equipment
- Lack of physical security over data communications closets or hubs or telecommunications equipment cabinets
- Location is in an area susceptible to environmental conditions such as contamination, electronic interference, extreme temperature and humidity, vermin, natural disasters, or power fluctuations

Systems Vulnerabilities

- Backup files and systems not available
- Complicated user interface (UI)
- Login banner leading to information that can expose the organization to unauthorized login access
- Inadequate firewall policies, network management, or resilience of routing
- Incorrect access rights
- Incorrectly configured or maintained application security features, operating system (OS), or security controls
- Lack of a firewall, an inventory of dial-up lines leading to inability to monitor dial-up access, application controls leading to fraudulent payments, change management software to enforce change management, dial back authentication, identification and authentication mechanisms, intrusion detection software, or logical access security
- Transmission of unencrypted confidential data
- Unencrypted communications
- Unprotected password tables

Administrative Vulnerabilities

- Failures in the change management process
- Inadequate control of software distribution, education of staff on software viruses, incident handling, information security policy, reporting and handling of software malfunctions, segregation of duties between software developers and operations staff, or software development standards
- Insufficient security training
- Lack of an industrial agreement, audit logs to detect unauthorized access, backups, communication between HR and IT groups for terminated employee notifications leading to terminated employees still having access to system, documentation, planning and implementation of communications cabling, or policies regarding dial-up access, modem use, and software use
- No business continuity plans or procedures for recovery of information and information assets
- Not keeping up to date with various online security organizations such as CERT
- Unclear obligations in outsourcing agreements
- Unclear or incomplete specifications
- Uncontrolled copying of data and/or software
- Use of shared Ethernet (for example, using Ethernet hubs instead of switches) so that all traffic is broadcast to any machine on a local segment

A threat is the potential cause, in one of many forms, of an unwanted event that may result in harm to information assets. Threats can be acts of nature, intentional or accidental. A threat could result in destruction of an asset, corruption or modification of an asset, theft, removal or loss of an asset, disclosure of an asset, use or acceptance of an illegal asset, or interruption of services.

Examples of Threats

The following list highlights examples of threats. These examples have been divided into categories for readability.

Physical and Environmental Threats

- Contamination
- Earthquake
- Electronic interference
- Extremes of temperature and humidity
- Power supply failure or fluctuations
- Fire
- Flood
- Storm
- Vermin
- Malicious destruction of data and facilities
- Building fire

Systems Threats

- Hackers
- Denial of Service (DoS) attacks
- Eavesdropping
- Industrial action
- Malicious code
- Masquerade
- Repudiation
- Sabotage
- Unauthorized data access, dial-in access, or software changes
- Failure of communications services or outsourced operations
- Misrouting/re-routing of messages
- Software/programming errors
- Technical failures
- Transmission errors

Administrative Threats

- Social engineering
- Theft and fraud
- Use of pirated software
- Web site intrusion

If a threat can trigger a vulnerability, the system is at risk. A threat would need to exploit the vulnerability in order to successfully cause harm.

Defining Risk

According to the ISO/IEC (2002) Guide 73, risk is defined as a “combination of the probability of an event and its consequences” and a “combination of the extent to which an occurrence of a particular set of circumstances is likely to occur and its outcome.” Risk is the potential that a given threat will exploit vulnerabilities to cause loss or damage to an asset or group of assets, and directly or indirectly affect the organization. The security risk level is determined from the combination of the asset values and assessed levels of related threats and associated vulnerabilities. Risk generally has three components:

- An event
- Probability of occurrence of the event
- Consequences of the event

There can be positive consequences, but generally when considering risk, organizations are looking at the potential negative events. And, it is worth noting that there can be more than one negative consequence that occurs from a negative event.

Cost-Benefit Analysis

The assigned monetary and qualitative value of information assets must be carefully determined to use as the basis for determining the cost/benefit of protecting the asset. A cost-benefit analysis for proposed new or enhanced controls includes consideration of the following:

- Determining the impact of implementing the new or enhanced controls (for example, monetary cost of the new control, reduced employee morale, and so on)
- Determining the impact of not implementing the new or enhanced controls (for example, lost sales because of lack of customer trust, or fines resulting from regulatory non-compliance)
- Estimating the costs of the implementation. Costs may include, but are not limited to:
 - 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. For example, an organization may determine after the cost-benefit analysis that it is best to implement expensive high-impact controls to a system with data classified as Top Secret, even though many of the controls would not be implemented if the same system contained non-sensitive data.

Identifying Assets at Risk

Assets include all the information and supporting items that an organization requires to conduct business. Examples of such assets include, but are not limited to:

- Information or data such as files containing payment details, voice records, image files, product information, manuals, and continuity plans
- Paper documents such as contracts and completed forms
- Software such as system software, application software, development tools, and utilities
- Physical equipment such as computer and communications equipment, magnetic media, other technical equipment such as medical equipment and environmental equipment, and furniture
- Services such as computing and communications services, service providers, and utilities
- People and their knowledge, including technical, operational, marketing, legal, and financial experts; contractors and consultants; and outsourced providers
- Image and reputation of the organization

Identifying Asset Values and Impacts

Organizations need to know asset values in order to identify the appropriate protection for assets and to determine the importance of the assets to the business. These values can be expressed in terms of the potential business impacts of negative events affecting loss of confidentiality, integrity, and/or availability. Potential impacts include financial losses and loss of revenue, market share, or image.

The dependencies of assets on other assets must also be considered because this dependence influences the values of the assets. For example, a seemingly less-important information system may require more protection if another mission-critical information system depends on the less-important system's results. Look at business continuity plans, process flow documentation, change control documentation, incident reports, and other types of documents to determine where such influences may exist. The values of assets with interdependencies may be considered and adjusted as follows, using data as the dependent assets, and software as the asset being considered:

- If the values of the dependent assets are lower or equal to the value of the asset considered, its value remains the same.
- If the values of the dependent assets are greater, the value of the asset considered should be increased according to the degree of dependency or the values of the other assets

As Figure 1.1 illustrates, all of the components of risk are related and must be considered within an effective risk management framework.



Figure 1: The components of risk must all be managed in an effective risk management framework.

Residual Risk

Organizations must manage risks and safeguard their operations to effectively manage and protect information assets. Some risks cannot be avoided completely; there will always be some residual risk. 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, or find an alternative, such as purchasing insurance. Once it has been determined that an acceptable level of risk has been achieved, the person responsible for risk management should sign a statement indicating acceptance of the residual risk prior to authorization or accreditation of the system for production operation. If the manager is professionally and/or legally held accountable by such a statement, there is a much greater chance that the manager will ensure that risk is reduced to the lowest practical level.

✍ Residual risk is the risk remaining after a decision is made to mitigate potential negative impact to an organization from identified vulnerabilities, threats, or attack probabilities.

What Is an Information Security Event?

In the context of information security risk, events are basically bad occurrences or incidents that cause trouble for business information and/or technology. An event is an incident or situation that occurs in a particular place during a particular interval of time.

BS7799/ISO 17799 provides useful examples of information security events. There are also unique events that are specific to each organization. For example, a large airline would have vastly different types of events than would a small health care provider clinic. However, with regard to information security, these two vastly different organizations would also have some events in common. Additionally, the occurrence of events would typically be reported to management; the more severe the event, the more quickly the event should be communicated. An advantage of having an information risk management program is that it will ensure the severity of many, if not all, events are determined before the event occurs, and by using a reasonable risk management framework, processes will be in place to report events.

Information security events that are likely to be common across many organizations include, but are not limited to:

- Theft
- Fraud
- Malicious code attack
- Acts of nature, vandals, and terrorists
- IT component failure
- Hacking
- DoS attacks
- Unauthorized disclosure
- Breaking the law
- Breach of contract

Determining Probability of an Event

To determine the likelihood, or probability, of an information security event, threats to an IT system must be analyzed along with the potential vulnerabilities and the controls in place for the IT system. This task cannot be accomplished with a great degree of accuracy, but doing such an analysis will reveal circumstances to help establish the amount of protection necessary for the asset, in addition to identifying the most threats and impacts possible for the asset. In general, probability is the likelihood of a specific outcome, measured by the ratio of specific outcomes to the total number of possible outcomes. Impact (also commonly referenced as consequence) refers to the magnitude of harm that could be caused by a threat's exploitation of vulnerability.



Impact is the outcome of an event expressed qualitatively or quantitatively, being a loss, injury, or disadvantage. There may be a range of possible outcomes associated with an event.

The level of impact is determined by the potential mission impacts and, in turn, produces a relative value for the IT assets and resources affected (such as the criticality and sensitivity of the IT system components and data). Asset values are used to identify the importance of the assets to the business, then determine the appropriate protection for assets. These values can be expressed in terms of the potential business impacts of undesirable events affecting loss of confidentiality, integrity, and/or availability. Potential impacts include financial losses, loss of revenue, or loss of market share or image.



Do not overlook unlikely events with severe impact, such as loss of life, facilities destruction, the failing of the organization, and so on.

Considering the Impacts of an Event

Unfortunately, it is futile to try to specifically and quantitatively determine the damage of an information security event by using a standard, repeatable, highly accurate method. The occurrence of an information security event may initiate several more impacts and may trigger other events. However, considering in general terms the consequences of an event is important to understanding and effectively assessing and addressing risks. Common information security event impacts that are common for most businesses include:

- Lost revenue
- Lost human and network resources because of unavailability
- Legal fees
- Customer dissatisfaction and lost customers
- Bad publicity
- Unanticipated costs
- Inability to carry out some or all of its business
- Loss of the monetary value of buildings and contents
- Failure to prosecute
- Court action against an employee or the business itself

Considering Likelihood and Impact

A detailed quantitative analysis is often conducted if a high level of risk is identified. Many organizations like to use tables showing likelihood of events based upon expected occurrences of the events. The following examples provide potential scales to use for a qualitative analysis. Organizations need to adjust the measures to suit the requirements of the risk analysis being conducted.

Measure	Description
Major	
Moderate	
Minor	
Insignificant	

Measure	Description
High	
Medium	
Possible	
Unlikely	


Measure	Description
High	Likely to threaten the effectiveness of the organization financially, legally and/or politically if not addressed.
Moderate	Likely to threaten running the organization, or organization services, and can be managed by implementing new or modified controls.
Low	Unlikely to threaten the organization and can be managed through routine controls.

Common Risk Reduction Models

Once an organization has identified risks, threats, vulnerabilities, assets, and impacts, a risk reduction plan must be implemented. Many risk reduction models already exist. It will save time for organizations to use these existing best practice examples of risk reduction models as a basis for their own risk management framework. Additionally, executives, especially those who don't want to be trailblazers, will more likely support the plan if a proven framework is used. Just a few of the existing models are discussed in the following sections.

Basel II

On June 26, 2004, a revised version of the original Basel Accord was released. This updated capital adequacy framework, referenced as Basel II, provides details for principally banking organizations to adopt risk-sensitive minimum capital requirements and reinforces the risk-sensitive requirements by detailing the principles for banks to use to assess the adequacy of their capital and for supervisors to use to review these assessments to ensure that banks have adequate capital to support their risks.

 Basel II text can be obtained from <http://www.bis.org/publ/bcbs107.htm>.

This framework includes an operational risk model that can serve all organizations well when incorporating information security risk into organizational risk management. Basel II defines operational risk as “the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk.”

COSO


The COSO ERM framework defines essential ERM components, discusses key ERM principles and concepts, suggests a common ERM language, and provides direction and guidance for ERM. The COSO framework is not specific to IT security risk management, but applies to the entire organizational and operational risk management issues.

 The COSO guide can be downloaded from <http://www.coso.org/>.

ISO Guide 73

The formal name for this risk management guide is PD ISO/IEC Guide 73:2002 Risk Management. This guide provides definitions for vocabulary associated with risk management with the intent of developing common understanding and consistent use of the terminology throughout the world. The intent of the guide is “to promote a coherent approach to the description of risk management activities and the use of risk management terminology.”

The guide encompasses the general field of risk management and includes basic terms related to people and organizations affected by risk, related to risk assessment, and related to risk treatment and control.

 The ISO Guide 73 can be purchased and downloaded from <http://www.bsi-global.com/Environmental/Risk/pdisoiec.xalter>.

NIST Special Publication 800-30


The National Institute of Standards and Technology (NIST) Risk Management Guide for Information Technology Systems provides guidelines that were created for use by United States federal organizations consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Appendix III. The guidelines provide a foundation for the development of a risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. The goal of the guidelines is to help organizations to better manage IT-related mission risks.

 NIST SP 800-30 can be downloaded from <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>. NIST also has draft library of controls based on a system’s sensitivity rating in NIST SP 800-53. You can view it at <http://csrc.nist.gov/publications/drafts.html#sp800-53>.

Prioritizing Risks

Performing a risk analysis should produce a risk profile that assigns a significance rating to each risk and provides a tool for prioritizing risk reduction (often called treatment) actions to give a view of the relative importance. Risk estimation can be quantitative, semi-quantitative, or qualitative in terms of the probability of occurrence and the possible consequence.


The process should map the risk to the business area affected, describe the primary control procedures in place, and indicate areas in which the level of risk control investment should be increased, decreased, or reapportioned. Making a position or department accountable for risk analysis will help to ensure that ownership of each risk is recognized and the appropriate management resources allocated.

 Risk evaluation should be used to make decisions about the significance of risks to the organization and to determine whether each specific risk should be accepted or treated.

Be Strategic When Managing Risk

Strategic information security risk management planning should accomplish the following objectives:

- Identify the specific risks the risk program will focus critical resources on managing. Determine the risk management capabilities (processes, investments, resources, and related activities) that will be required. Determine how the resources will be coordinated across the enterprise.
- Determine how the risk program will measure the results and demonstrate the value of risk management processes, investments, resources, and related activities.
- Determine the goals of the risk program. Document how the risk program will benefit the organization and the key stakeholders.

 Challenges to managing risk include, but are not limited to:
Getting adequate budget, people, and tools necessary to do the job
Acquiring visible executive management support

Developing a well thought out strategic information security risk management plan will provide many organizational benefits:

- Information gathering during strategic planning will provide an excellent opportunity to interview and receive input from enterprise leaders while allowing them to participate in the development of the risk program and buy into the outputs of the strategic plan.
- Enables the organization to rationalize current and future activities, investments, and hiring plans
- Enforces professionalism and discipline around the budgeting process
- Provides a way to communicate the vision for the risk program to staff, team, partners, management, and other key stakeholders
- Demonstrates due-diligence
- Reduces potential political decisions

Building a Risk Management Roadmap

The strategic information security risk management plan should create a business case and a roadmap for your risk program and provide for an ongoing, sustainable process. To do so effectively:

- Establish context and scope—Set parameters for the risk program and for the planning process: What risks will be covered? What parts of the risk management process will be involved? Which business units? Which locations? What are the risk management program goals?
- Assess the current state—Clearly describe where the risk program currently stands. Where is the organization today? What is working now and what isn't with the way the organization currently manages risk? What has changed in the risk and business environment that necessitates a change in the risk program? What are peer organizations doing?
- Look to the future—Articulate where the risk program needs to be and why. Where do you need to be? What are the stakeholder needs and expectations? What will the risk program look like and what will it be able to do? How will this benefit the organization? What are the consequences to your organization if you don't do these things?
- State goals and initiatives—Document what the risk program is there to achieve and how it will get there. What are the objectives for the risk program? What is the risk program trying to accomplish, change, or affect? What initiatives or projects will get the organization to those objectives? How much will they cost? What are the ongoing costs? What are the benefits?
- Frame the implementation—Lay out a roadmap for implementation of the risk program. In what sequence will the projects occur? Which needs to happen first? When will they begin and end? How will they rollout across your organization? Who will perform the projects? What are the quick wins?
- Measure performance—Demonstrate the value of the risk program. How will success be measured? Where does the organization currently stand? Where does the organization need to be in 6 months, 1 year, or even 5 years in order to achieve the stated goals? How often and in what manner will the results be reported to the risk program's stakeholders?

Integrating Information Security Risk Management into the Enterprise

Information security risk management programs should effectively collaborate across the enterprise and have a direct connection to the strategic planning process as well as the critical projects, initiatives, business units, and business functions. Broad, comprehensive integration of risk management programs across the organization lead to more effective and efficient business programs.

Using Qualitative and Quantitative Measures

Most organizations will progress from being able to qualitatively assess information security risks to being able to quantify the risks. Generally, the more quantifiable the information about the risk, the more risk reduction options available to the organization. To determine the acceptable level of risk, answer the following questions:


- Where should limited time and resources be allocated to minimize risk exposures? Why?
- What level of risk exposure requires immediate action? Why?
- What level of risk requires a formal response strategy to mitigate the potentially significant impact? Why?
- What events have occurred in the past and at what level were they managed? Why?

Always provide the answer to the why questions to document the quantitative and/or qualitative basis for the answer; otherwise, the decision will not be justified and will appear arbitrary.

Identifying Business Drivers

Business drivers create value for stakeholders. Business drivers vary by industry; however, they will generally fall into four categories:

- **Managing growth**—Increasing revenue or improving the top line is achieved in many ways, such as expanding into new markets, expanding overseas, extending existing product lines, developing new product areas, and reaching new customer segments.
- **Driving innovation**—The ability to create new products and markets through product innovativeness, product development, and so on.
- **Controlling costs**—Effectively managing cost increases the competitive positioning of the business and increases available budget dollars.
- **Allocating capital**—Capital should be effectively allocated to those business units, initiatives, markets, and products that will have the highest return for the least risk. These are the primary business drivers.

 A clear understanding and ability to speak about your value drivers will help you bridge the communication gap that typically exists between information security risk managers and senior management.

Identifying Risk Drivers

Consider both the types of risk and the capability of the organization to manage those risks:

- Risk types—Develop a risk classification or categorization to create a common nomenclature that facilitates discussions about risk issues within the organization and facilitates the development of information systems that gather, track, and analyze information about various risks, including the ability to correlate cause and effect, identify interdependencies, and track budgeting and loss of experience information.
- Risk capability—The ability of the organization to absorb and manage various risks. This type of risk includes how well the various risk management–related groups work together, what the risk process is within the enterprise, what organizational cultural elements should be considered, and so on.

Establishing Metrics

Accurate and timely creation of metrics is critical to the success of the risk management program. Connect the risk management programs to other existing business management metrics. Provide feedback about both the internal business processes and external outcomes to continuously improve strategic performance and results. For some excellent examples of metrics, see NIST SP 800-55, Security Metrics Guide for Information Technology Systems (<http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf>).

Providing Training

Establish effective training programs to ensure that risk management programs are effectively integrated into regular business processes. For example, strategic planners, responsible for the strategic planning process, need constant reinforcement regarding the risk assessment processes.

Providing Continuous Communication

Provide frequent and consistent communications around the purpose, success, and cost of the risk management program to maintain management support and to continually obtain necessary participation of managers and line personnel in the ongoing risk management program.

Using Appropriate Tools

Evaluate, purchase or develop appropriate tools to enhance the effectiveness of the risk management capability. Many commercial tools are available and their utility across a range of risk management activities should be considered as appropriate within the organization.

Integrating Risk Management Into The System Development Life Cycle

Risk management is an iterative process. Risk management activities are relevant to every phase of the system development life cycle (SDLC). An IT SDLC generally has five phases, each of which are explored in the following sections.

Phase 1: Project Initiation

The need for a new IT system, or IT system update, is identified, 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 updated. The risks identified during this phase can be used to support the security analyses of the IT system. Such analysis will lead to acceptance of risks or determination of how to reduce risk levels to acceptable levels.

Phase 3: Implementation


The system security features are configured, enabled, tested, and verified. The risk management process is used to assess the system implementation against security requirements and the modeled operational environment. Decisions regarding risks identified during this phase must be made prior to system operation.

Phase 4: Operation or Maintenance

The system is placed into production. The system is 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 re-accreditation, and whenever major changes, as defined by the organization, are made in the IT system operational or production environment.


Phase 5: Disposal

The disposal phase may involve the disposal of information, hardware, and/or 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 destroyed, that residual data is appropriately handled, and that system migration is conducted in a secure and consistent manner.

 If risk management is not an integral part of all phases of the IT SDLC, the organization may need to redesign a system, or accept what would typically be unacceptable risks because redesigning the system is too expensive.

The Information Security Risk Management Methodology

Risk assessment is the first process in the risk management methodology and can be used to determine the extent of the potential threat and the risk associated with an IT system throughout its SDLC. The output helps to identify appropriate controls for reducing risk during the risk mitigation process.

 The most effective risk assessments identify, classify, and articulate the likelihood and impact of risks, then address the current ability of the organization to manage those risks.

There are generally nine steps within the risk assessment process. The following sections explore each of these steps.

Step 1: System Characterization

Define the scope and activities of security related-interest including all system boundaries, information, and resources that will make up the domain of assessment. At a minimum, this definition includes 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. In addition, this step involves identifying the system owner (the person responsible for the system, not necessarily the one who supplies the funding). The owner will be able to answer many questions and should be able to determine system and data criticality, system boundaries, and so on. In some instances, the risk assessment will make the system owner realize and understand their responsibilities as the owner.

Step 2: Threat Identification

Identify potential threat sources and compile a threat statement listing potential threat-sources that are applicable to the IT system being evaluated. Consider using a standard list of threats for your organization to help the participants in the risk assessment to consider all possible threats. Use the one provided earlier as a starting point.

Step 3: Vulnerability Identification

Perform an analysis of the vulnerabilities associated with the system environment. Develop a list of system, application, and process vulnerabilities that could be exploited by the potential threat sources. We explored examples of such vulnerabilities earlier.

Step 4: Control Analysis

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 system vulnerability.

Step 5: Likelihood Determination

Derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment. For example, consider using High, Medium, and Low ratings as provided in the earlier example. Establish a rating appropriate for the organization that will be used consistently throughout all risk assessments. Do not select a rating system that is too granular; otherwise, there will likely be needless time and effort spent distressing over shades of gray. Use the following governing factors:

- Threat source motivation and capability
- Nature of the vulnerability
- Existence and effectiveness of current and planned controls

Step 6: Impact Analysis

Determine the adverse impact resulting from a successful threat exercise of vulnerability. The adverse impact of a security event can be described in terms of loss or degradation of any or a combination.

Step 7: Risk Determination

Assess the level of risk to the IT system. Determine risk for each particular threat/vulnerability pair by considering:

- The likelihood of a given threat source to exercise a given vulnerability
- The magnitude of the impact if a threat source successfully exercises the vulnerability
- The adequacy of planned or existing security controls for reducing or eliminating risk

Step 8: Control Recommendations

Provide controls to mitigate or eliminate the identified risks, as appropriate to the organization's operations to reduce the level of risk to the IT system and the associated data to an acceptable level. When recommending controls consider:

- Effectiveness of recommended options
- Legislation and regulation
- Organizational policy
- Operational impact
- Safety and reliability

☞ Various risk management functions must participate, exchange information and processes, and cooperate on risk mitigation activities. A risk assessment should include a review of the interactions, sharing of information, collaborative approach to managing risk, and so on that exists among the various risk management functions. Some of these risk management functions might include business continuity planning, internal audit, insurance, crisis management, privacy, physical security, legal, information security, and credit risk management.

Step 9: Results Documentation

Document results in a report or briefing. An effective risk assessment report helps senior management make decisions on policy, procedural, budget, and system operational and management changes. 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. Determine a central location to store the reports, document who has access to them, and document how the reports will be protected from unauthorized access.

Mitigating Risk

Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process. Elimination of all risk is impractical and impossible to achieve. Senior management and functional and business managers must implement the most appropriate controls to decrease risks to an acceptable level, with minimal adverse impact on the organization's resources and mission. Risk management must be cost-effective.

☞ Reduce risk exposure time through process-focused capabilities to minimize the time taken to both discover and resolve security issues from months down to days, or even minutes, reducing exposure to threats and vulnerabilities. Be sure to provide the right level of risk reduction to demonstrate due care and that will visibly demonstrate risk reduction. Monitor all factors that affect risk and indicate security effectiveness. Follow an ongoing sustainable, documented, repeatable process for reducing and reporting risks. Hold managers accountable for following the process. The more applied the risk mitigation process, the better.

Risk mitigation can be achieved systematically through one or a combination of the following risk mitigation options:

- Risk assumption—Accepting the potential risk and continuing to operate the IT system or implementing controls to lower the risk to an acceptable level.
- Risk avoidance—Avoiding the risk by eliminating the risk cause and/or consequence. For example, if it is too expensive to protect dial-in modems with additional controls, it may be best to remove the dial-in modems.
- Risk limitation—Limiting risk by implementing controls that minimize the adverse impact of a threat that exercises vulnerability.
- Risk planning—Managing risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls.
- Research and acknowledgment—Lowering the risk of loss by acknowledging the vulnerability and researching controls to correct the vulnerability.
- Risk transference—Transferring the risk by using other options to compensate for the loss, such as purchasing insurance. Risk transference is usually chosen when all other options are unacceptable or not possible.

Information Security Risk Management Strategy

Develop an information security risk management strategy that focuses management attention on both risk strategy for particular types of risks as well as the enterprise risk management program strategy. Key points to remember when creating the information security risk strategy include:

- Understand risk to the business and to IT systems
- Understand the business drivers of the organization
- Develop, or promote the development of, classification systems for categorizing risks
- Analyze what is not covered in insurance coverage
- Relate IT risk to enterprise risk
- Determine acceptable risk
- Understand the criticality of the network and data
- Create an organizational security position index
- Effectively report risk
- Address risks

The process of producing the risk management roadmap can be described in terms of a series of steps.

Step 1: Identify Events

Name each risk event and briefly describe it. Use the list of information security events listed earlier as a starting point, then add to it based upon the unique organizational environment.

Step 2: Identify Assets

Start with a generic list that includes the items listed earlier. Add to this list and otherwise modify it as necessary, the idea being to derive the assets that require protection from the analysis rather than the other way round (which, unfortunately, is the typical way of carrying out a risk assessment). Use business continuity planning, acquisition, and other business processes to help identify the assets.

Step 3: Identify Threats

Choose from the list of threats described earlier and add to them with organization-specific threats as applicable.

Step 4: Identify Impacts

Start with the standard impacts described earlier and add to them with organization-specific impacts as required.

Step 5: Produce Risk Reduction Plans

Produce a risk-reduction plan for each identified risk event. Repeat the following steps until all the impacts have been addressed:

- Identify the risks leading to each impact for known threats
- Identify the risks leading to each impact for unknown, but possible, threats
- Address unacceptable residual risks
- Incorporate the controls and make the control structure as functional as possible

Step 6—Follow Up and Verify that Actions Have Occurred

Once all the risk treatment plans have been developed, do some verification to ensure that nothing has been overlooked; ensure that

- All the assets in the asset inventory have been used and risk reduction activities applied. If any are left over, document why they were not used and remove them from the inventory if applicable.
- All the impacts in the impact list have been addressed.
- All the threat agents in the threat list have been addressed.
- All event-impact pairs have been addressed.
- All risks are identified as being an acceptable or unacceptable risk, and document why.
- All control failures have been considered and addressed.
- All unacceptable residual risks have been addressed and identified improvements or compensating controls have been implemented.

In addition, show the report to system owners and personnel for their feedback. They may identify mistakes in the report, and it will be a way to raise their awareness of the systems for which they are responsible.

Summary

Risk management is a central part of every organization's strategic management. Crucial to implementation of a successful information security risk management program is the ability to identify and protect critical information assets based upon the business mission and goals. A successful information security risk management program is the enabler needed to make the implementation successful.

Risk management should be a continuous and developing process that runs throughout the organization's strategy and the implementation of that strategy. It should methodically address all the risks surrounding the organization's activities past, present, and future. It must be integrated into the culture of the organization with an effective policy and a program by the most senior management. It must translate the information security strategy into tactical and operational objectives, assigning responsibilities throughout the organization with each manager and employee responsible for the management of risk as part of their job description. It must support accountability, performance measurement, and reward, resulting in improving operational efficiency at all levels.

The successful management of information security projects continues to increase in strategic significance for the competitiveness of organizations. IT is an essential part of most projects. Even traditional business processes cannot survive without electronic data processing. The risks connected with the implementation of IT projects constitute a substantial part of the operational risks within an enterprise.