**RISK MANAGEMENT**

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. This guide provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. The ultimate goal is to help organizations to better manage IT-related mission risks.

**IMPORTANCE OF RISK MANAGEMENT**

Risk management encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment. Section 3 of this guide describes the risk assessment process, which includes identification and evaluation of risks and risk impacts, and recommendation of risk-reducing measures. Section 4 describes risk mitigation, which refers to prioritizing, implementing, and maintaining the appropriate risk-reducing measures recommended from the risk assessment process. Section 5 discusses the continual evaluation process and keys for implementing a successful risk management program. The DAA or system authorizing official is responsible for determining whether the remaining risk is at an acceptable level or whether additional security controls should be implemented to further reduce or eliminate the residual risk before authorizing (or accrediting) the IT system for operation.

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.

The head of an organizational unit must ensure that the organization has the capabilities needed to accomplish its mission. These mission owners must determine the security capabilities that

their IT systems must have to provide the desired level of mission support in the face of realworld threats. Most organizations have tight budgets for IT security; therefore, IT security spending must be reviewed as thoroughly as other management decisions. A well-structured risk management methodology, when used effectively, can help management identify appropriate controls for providing the mission-essential security capabilities.

**INTEGRATION OF RISK MANAGEMENT INTO SDLC**

Minimizing negative impact on an organization and need for sound basis in decision making arevthe fundamental reasons organizations implement a risk management process for their ITvsystems. Effective risk management must be totally integrated into the SDLC. An IT system’svSDLC has five phases: initiation, development or acquisition, implementation, operation or

maintenance, and disposal. In some cases, an IT system may occupy several of these phases at the same time. However, the risk management methodology is the same regardless of the SDLC phase for which the assessment is being conducted. Risk management is an iterative process that can be performed during each major phase of the SDLC. Table 2-1 describes the characteristics of each SDLC phase and indicates how risk management can be performed in support of each.



**KEY ROLES**

Risk management is a management responsibility. This section describes the key roles of the personnel who should support and participate in the risk management process.

* **Senior Management.** Senior management, under the standard of due care and ultimate responsibility for mission accomplishment, must ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the mission. They must also assess and incorporate results of the risk assessment activity into the decision making process. An effective risk management program that

assesses and mitigates IT-related mission risks requires the support and involvement of senior management.

* **Chief Information Officer (CIO).** The CIO is responsible for the agency’s IT planning, budgeting, and performance including its information security components. Decisions made in these areas should be based on an effective risk management program.
* **System and Information Owners.** The system and information owners are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of the IT systems and data they own. Typically the system and information owners are responsible for changes to their IT systems. Thus, they usually have to approve and sign off on changes to their IT systems (e.g., system enhancement, major changes to the software and hardware). The system and information owners must therefore understand their role in the risk management process and fully support this process.
* **Business and Functional Managers.** The managers responsible for business operations and IT procurement process must take an active role in the risk management process. These managers are the individuals with the authority and responsibility for making the trade-off decisions essential to mission accomplishment. Their involvement in the risk management process enables the achievement of proper security for the IT systems, which, if managed properly, will provide mission effectiveness with a minimal expenditure of resources.
* **ISSO.** IT security program managers and computer security officers are responsible for their organizations’ security programs, including risk management. Therefore, they play a leading role in introducing an appropriate, structured methodology to help identify, evaluate, and minimize risks to the IT systems that support their organizations’ missions. ISSOs also act as major consultants in support of senior management to ensure that this activity takes place on an ongoing basis.
* **IT Security Practitioners.** IT security practitioners (e.g., network, system, application, and database administrators; computer specialists; security analysts; security consultants) are responsible for proper implementation of security requirements in their IT systems. As changes occur in the existing IT system environment (e.g., expansion in network connectivity, changes to the existing infrastructure and organizational policies, introduction of new technologies), the IT security practitioners must support or use the risk management process to identify and assess new potential risks and implement new security controls as needed to safeguard their IT systems
* **Security Awareness Trainers (Security/Subject Matter Professionals).** The organization’s personnel are the users of the IT systems. Use of the IT systems and data according to an organization’s policies, guidelines, and rules of behavior is critical to mitigating risk and protecting the organization’s IT resources. To minimize risk to the IT systems, it is essential that system and application users be provided with security awareness training. Therefore, the IT security trainers or security/subject matter professionals must understand the risk management process so that they can develop appropriate training materials and incorporate risk assessment into training programs to educate the end users.

**RISK ASSESSMENT**

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, as discussed in Section 4.

***Risk*** is a function of the ***likelihood*** of a given ***threat-source’s*** 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, which are described below this:

* • Step 1System Characterization (Section 3.1)
* • Step 2Threat Identification (Section 3.2)
* • Step 3Vulnerability Identification (Section 3.3)
* • Step 4Control Analysis (Section 3.4)
* • Step 5Likelihood Determination (Section 3.5)
* • Step 6Impact Analysis (Section 3.6)
* • Step 7Risk Determination (Section 3.7)
* • Step 8Control Recommendations (Section 3.8)
* • Step 9Results Documentation (Section 3.9).

Steps 2, 3, 4, and 6 can be conducted in parallel after Step 1 has been completed. Figure 3-1 depicts these steps and the inputs to and outputs from each step.



**STEP 1: SYSTEM CHARACTERIZATION**

In assessing risks for an IT system, the first step is to define the scope of the effort. In this step, the boundaries of the IT system are identified, along with the resources and the information that constitute the system. Characterizing an IT system establishes the scope of the risk assessment effort, delineates the operational authorization (or accreditation) boundaries, and provides

information (e.g., hardware, software, system connectivity, and responsible division or support personnel) essential to defining the risk.

Section 3.1.1 describes the system-related information used to characterize an IT system and its operational environment. Section 3.1.2 suggests the information-gathering techniques that can be used to solicit information relevant to the IT system processing environment. The methodology described in this document can be applied to assessments of single or multiple, interrelated systems. In the latter case, it is important that the domain of interest and all interfaces and dependencies be well defined prior to applying the methodology.

**System-Related Information**

Identifying risk for an IT system requires a keen understanding of the system’s processing environment. The person or persons who conduct the risk assessment must therefore first collect system-related information, which is usually classified as follows:

* Hardware
* Software
* System interfaces (e.g., internal and external connectivity)
* Data and information
* Persons who support and use the IT system
* System mission (e.g., the processes performed by the IT system)
* System and data criticality (e.g., the system’s value or importance to an organization)
* System and data sensitivity.*4*
* Additional information related to the operational environmental of the IT system and its data includes, but is not limited to, the following:
	+ The functional requirements of the IT system
	+ Users of the system (e.g., system users who provide technical support to the IT
	+ system; application users who use the IT system to perform business functions)
	+ System security policies governing the IT system (organizational policies, federal requirements, laws, industry practices)
	+ System security architecture

Current network topology (e.g., network diagram)

* + Information storage protection that safeguards system and data availability, integrity, and confidentiality
	+ Flow of information pertaining to the IT system (e.g., system interfaces, system input and output flowchart)
	+ Technical controls used for the IT system (e.g., built-in or add-on security product that supports identification and authentication, discretionary or mandatory access control, audit, residual information protection, encryption methods)
	+ Management controls used for the IT system (e.g., rules of behavior, security planning)
	+ Operational controls used for the IT system (e.g., personnel security, backup, contingency, and resumption and recovery operations; system maintenance; off-site storage; user account establishment and deletion procedures; controls for segregation of user functions, such as privileged user access versus standard user access)
	+ Physical security environment of the IT system (e.g., facility security, data center policies)
	+ Environmental security implemented for the IT system processing environment (e.g., controls for humidity, water, power, pollution, temperature, and chemicals).

For a system that is in the initiation or design phase, system information can be derived from the design or requirements document. For an IT system under development, it is necessary to define key security rules and attributes planned for the future IT system. System design documents and the system security plan can provide useful information about the security of an IT system that is in development.

For an operational IT system, data is collected about the IT system in its production environment, including data on system configuration, connectivity, and documented and undocumented procedures and practices. Therefore, the system description can be based on the security provided by the underlying infrastructure or on future security plans for the IT system.

**Information-Gathering Techniques**

Any, or a combination, of the following techniques can be used in gathering information relevant to the IT system within its operational boundary:

• **Questionnaire.**

To collect relevant information, risk assessment personnel can develop a questionnaire concerning the management and operational controls planned

or used for the IT system. This questionnaire should be distributed to the applicable technical and nontechnical management personnel who are designing or supporting the IT system. The questionnaire could also be used during on-site visits and interviews.

• **On-site Interviews.**

Interviews with IT system support and management personnel can enable risk assessment personnel to collect useful information about the IT system (e.g., how the system is operated and managed). On-site visits also allow risk

assessment personnel to observe and gather information about the physical,

environmental, and operational security of the IT system. Appendix A contains sample interview questions asked during interviews with site personnel to achieve a better understanding of the operational characteristics of an organization. For systems still in the design phase, on-site visit would be face-to-face data gathering exercises and could provide the opportunity to evaluate the physical environment in which the IT system will operate.

• **Document Review.**

Policy documents (e.g., legislative documentation, directives), system documentation (e.g., system user guide, system administrative manual, system design and requirement document, acquisition document), and security-relateddocumentation (e.g., previous audit report, risk assessment report, system test results, system security plan*5*, security policies) can provide good information about the security controls used by and planned for the IT system. An organization’s mission impact analysis or asset criticality assessment provides information regarding system and data criticality and sensitivity.

• **Use of Automated Scanning Tool.**

Proactive technical methods can be used to collect system information efficiently. For example, a network mapping tool can identify the services that run on a large group of hosts and provide a quick way of building individual profiles of the target IT system(s).

Information gathering can be conducted throughout the risk assessment process, from Step 1

(System Characterization) through Step 9 (Results Documentation).

***Output from Step 1******Characterization of the IT system assessed, a good picture of the IT***

***system environment, and delineation of system boundary***

**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 canbe 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 (Section 3.5), one must consider threat-sources, potential vulnerabilities (Section 3.3),and existing controls (Section 3.4).

**1. Threat-Source Identification**

The goal of this step is to identify the potential threat-sources and compile a threat statemen listing potential threat-sources that are applicableto the IT system being evaluated.

A threat-source is defined as any circumstance or event with thepotential to cause harm to an IT system. The common threatsources can be natural, human, or environmental. In assessing threat-sources, it is important to consider all potential threat-sources that could cause harm to an IT system and its processing environment. For example, although the threat statement for an IT system located in a desert may not include “natural flood” because

of the low likelihood of such an event’s occurring, environmental threats such as a bursting pipe can quickly flood a computer room and cause damage to an organization’s IT assets and resources. Humans can be threat-sources through intentional acts, such as deliberate attacks by malicious persons or disgruntled employees, or unintentional acts, such as negligence and errors.

A deliberate attack can be either (1) a malicious attempt to gain unauthorized access to an IT system (e.g., via password guessing) in order to compromise system and data integrity, availability, or confidentiality or (2) a benign, but nonetheless purposeful, attempt to circumvent system security. One example of the latter type of deliberate attack is a programmer’s writing a Trojan horse program to bypass system security in order to “get the job done.”

**2 Motivation and Threat Actions**

Motivation and the resources for carrying out an attack make humans potentially dangerous threat-sources. Table 3-1 presents an overview of many of today’s common human threats, their possible motivations, and the methods or threat actions by which they might carry out an attack.

This information will be useful to organizations studying their human threat environments and customizing their human threat statements. In addition, reviews of the history of system breakins; security violation reports; incident reports; and interviews with the system administrators, help desk personnel, and user community during information gathering will help identify human threat-sources that have the potential to harm an IT system and its data and that may be a concern where a vulnerability exists. An estimate of the motivation, resources, and capabilities that may be required to carry out a successful attack should be developed after the potential threat-sources have been identified, in order to determine the likelihood of a threat’s exercising a system vulnerability, as described in Section 3.5.

The threat statement, or the list of potential threat-sources, should be tailored to the individual organization and its processing environment (e.g., end-user computing habits). In general, information on natural threats (e.g., floods, earthquakes, storms) should be readily available.

Known threats have been identified by many government and private sector organizations.

Intrusion detection tools also are becoming more prevalent, and government and industry organizations continually collect data on security events, thereby improving the ability to realistically assess threats. Sources of information include, but are not limited to, the following: Intelligence agencies (for example, the Federal Bureau of Investigation’s National

Infrastructure Protection Center)

Federal Computer Incident Response Center (FedCIRC)

Mass media, particularly Web-based resources such as SecurityFocus.com,

SecurityWatch.com, SecurityPortal.com, and SANS.org.

***Output from Step 2******A threat statement containing a list of threat-sources that could exploit***

***system vulnerabilities***



**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. Recommended methods for identifying system vulnerabilities are the use of vulnerability sources, the performance of system security testing, and the development of a security requirements checklist.

It should be noted that the types of vulnerabilities that will exist, and the methodology needed to determine whether the vulnerabilities are present, will usually vary depending on the nature of the IT system and the phase it is in, in the SDLC:

* If the IT system has not yet been designed, the search for vulnerabilities should focus on the organization’s security policies, planned security procedures, and system requirement definitions, and the vendors’ or developers’ security product analyses (e.g., white papers).
* If the IT system is being implemented, the identification of vulnerabilities should be expanded to include more specific information, such as the planned security features described in the security design documentation and the results of system certification test and evaluation.
* If the IT system is operational, the process of identifying vulnerabilities should include an analysis of the IT system security features and the security controls, technical and procedural, used to protect the system





Sumber:

Gary Stonebumer, Alice Goguen, and Alexis Fringa, Risk Management Guide for IS.

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf