IJCSC International Journal of Computer Science & Communication Vol. 1, No. 1, January-June 2010, pp. 33-38

Risk Management Process for Information Security System

S. P. Datta

Eastern Institute of Management, Kalyani University, India;

e-mail: sp_datta2000@yahoo.co.in

Prof. Pranab Banerjee, Electronics & Telecom. Engg., Jadavpur University, India.

ABSTRACT

An appropriate risk management process is an extremely critical component of a successful information security program. The main objective of an organization's risk management process is to secure the organization's ability to perform its business mission, and not only its information assets. Hence, the risk management process cannot be considered only as a technical function performed by the information security experts, but need to be seen as an essential management function of the organization that is tightly integrated into the system development life cycle (SDLC). As risk cannot be eliminated completely, the risk management practices and procedures to be appropriately adopted that would allow information security officers to balance the operational benefits and economic costs of protective measures, and achieve gains in mission.

1. INTRODUCTION

An effective risk management process is an important component of a successful information security program. The objective of an organization's risk management process is to protect the organization and its ability to perform its mission, not just its information assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the information security experts who operate and manage the information security system, but as an essential management function of the organization that is tightly integrated into the system development life cycle (SDLC)[1], as depicted in Figure 1.

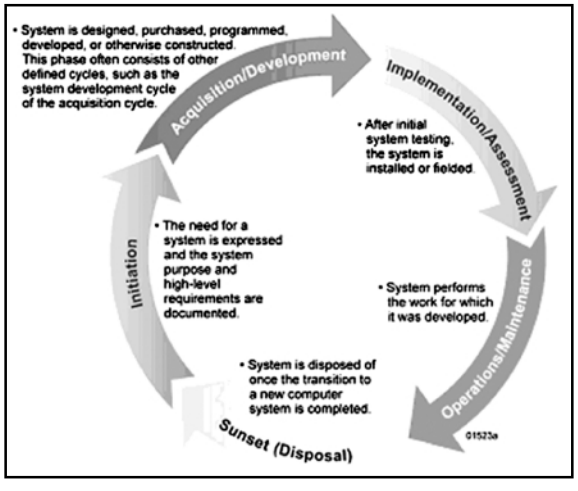

Fig 1: System Development Life Cycle (SDLC)

Risk management encompasses three processes: risk assessment, risk mitigation, and evaluation & assessment. Because the risk can't be eliminated entirely, the risk management process allows information security program managers to balance the operational and economic costs of protective measures and achieve gains in mission capability. By employing practices and procedures designed to foster informed decision making, agencies help protect their information systems and the data (by maintaining confidentiality, integrity and availability of information) that support their own mission.

2. OVERVIEW

Information system security processes and activities provide valuable input into managing IT systems and their development, enabling risk identification, planning and mitigation. A risk management approach involves continuously balancing the protection of agency information and assets with cost of security controls and mitigation strategies throughout the complete "information system development life cycle". The most effective way to implement risk management is to identify systematically critical assets and operations, as well as vulnerabilities across the agency.

'Risk' is the impact of the realized 'threat' on a 'vulnerability' (of an organization) as per the following 'risk' equation:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Event Cost}.$$

Threat is the likelihood that a particular vulnerability will be successfully attacked over a certain period.

Vulnerability is any weakness in a given system (including hardware, software, administrative controls, and associated processes and procedures) whose (intentional or accidental) exploitation leads to a violation

of security policy or an adverse impact on an asset, as well as any non-compliance with any mandated information security requirements.

Event cost is the quantum value of the loss that is incurred if the vulnerability is successfully exploited.

One of the things that makes risks so difficult to deal with is its uncertainty. That is why it is referred to as risk. Risk management is an aggregation of three processes[2], [3]:

- *Risk Assessment:* Assessment of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence.
- *Risk Mitigation:* When a combination of threat, vulnerability, and cost combine to create a non-trivial risk for a particular class of asset, that risk is fed into the next phase of risk mitigation process for developing controls to minimize or eliminate security risks that may affect information systems, for an acceptable cost.
- *Evaluation & Assessment:* Today, information technology environments are continuously evolving. So, it becomes important to carry out periodic reviews of security risks and implemented controls to take account of changes to business requirements and priorities, and also new threats and vulnerabilities.

If applied appropriately with due diligence, this process meets the requirements of "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems" collected by and used by the organization, and "ensuring that information security management processes are integrated with agency strategic and operational planning processes".

2.1. Risk Assessment

To understand the risk assessment process, it is essential to define the term risk[3] as "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." The goal of the risk assessment process is to identify and assess the risks to a given environment. The depth of the risk assessment performed can vary greatly and is determined by the criticality and sensitivity of the system, as applied to confidentiality, integrity, and availability[4], To meet the goal of the risk assessment, a nine-step process is defined in NIST SP 800-30. To simplify the process somewhat, the nine-step process described in NIST SP 800-30 is reduced to a six- step process, whereby Steps 4, 5, and 6 of the process are combined to create the Risk Analysis step as indicated in Figure 2.

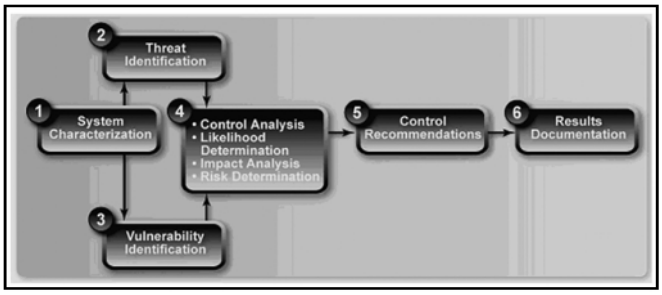

Fig 2: Risk Assessment Process

The likelihood of a given threat successfully exploiting a given vulnerability is estimated by evaluating the threat source's motivation, opportunity, and methods for conducting such an exploitation. The impact of a successful exploitation is estimated through an analysis of the effect the exploitation can have on the confidentiality, integrity, and availability of the system and the data it processes. The determination of the criticality and sensitivity of the system, in terms of its confidentiality, integrity, and availability, is found by applying the concepts and processes discussed in detail within FIPS 199.

The risk assessment process is usually repeated at least every three years for federal agencies. However, risk assessments should be conducted and integrated into the SDLC for information systems, not because it is required by law or regulation, but because it is a good practice and supports the organization's business objectives or mission.

2.1.1. System Characterization

Characterizing an information 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). This step begins with the identification of the information system boundaries, resources, and information.

When characterizing the system, the mission criticality and sensitivity (as previously identified using FIPS 199 to determine the system's appropriate security categorization) are described in sufficient terms to form a basis for the scope of the risk assessment. For example, a system determined to be of low impact may not require hands-on security testing and evaluation. Various techniques, such as questionnaires, interviews, documentation reviews, and automated scanning tools, can be used to collect the information needed to fully characterize the system. At a minimum, the system

characterization describes following individual system components:

- Hardware (hardware and OS for every individual server, workstation, terminal, etc);
- Software (RDBMS, Web Server, Internet Info. Server, etc);
- Interface (external) to other systems;
- Data; and
- People.

System characterization also describes other factors with the potential to affect the security of the system, like:

- System functional requirements;
- Organizational security policy and architecture;
- System network topology;
- Information flows throughout the system;
- Management, operational, technical security controls implemented or planned;
- Physical and environmental security mechanisms.

2.1.2. Threat Identification

Threat identification consists of identifying threat sources with the potential to exploit weaknesses in the system. This step should culminate in the development of a "threat statement," or a comprehensive listing of potential threat sources. The threat statement must be tailored to the individual organization and its processing environment, which is accomplished by performing a threat evaluation, using the system characterization as the basis, for the potential to cause harm to the system.

There are common threat sources that typically apply, regardless of the system, that should be evaluated. These common threats can be categorized into three areas: (a) natural threats (e.g., floods, earthquakes, tornadoes, landslides, avalanches, electrical storms), (b) human threats (intentional or unintentional), and (c) environmental threats (e.g., power failure). In general, information on natural threats (e.g., floods, earthquakes, storms) should be readily available. 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;
- United States Computer Emergency Readiness Team (US-CERT); and
- Mass media, including Web-based resources.

2.1.3. Vulnerability Identification

Vulnerability is defined as "a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy"[3]. Vulnerabilities can be identified using a combination of a number of techniques and sources. Reviews of such sources as previous risk assessments, audit reports, vulnerability lists [e.g., NIST National Vulnerability Database (NVD), found at nvd.nist.gov], and security advisories can be used to begin the process of vulnerability identification. System security testing, using methods such as automated vulnerability scanning tools; security, test, and evaluation (ST&E); and penetration testing can be used to augment the vulnerability source reviews and identify vulnerabilities that may not have been previously identified in other sources.

Developing a security requirements checklist based on the security requirements specified for the system during the conceptual, design, and implementation phases of the SDLC can be used to provide a 360-degree inspection of the system[5]. Complete care to be taken to ensure the inclusion of appropriate questions in the areas of management, operational, and technical security controls. The results of the checklist (or questionnaire) can be used as input for evaluating compliance and noncompliance, which in turn identifies system, process, and procedural weaknesses that represent potential vulnerabilities.

2.1.4. Risk Analysis

The risk analysis is an estimation of risk to the system, an analysis that requires the consideration of closely interwoven factors, such as the security controls in place for the system under review, the likelihood that those controls will be either insufficient or ineffective protection of the system, and the impact of that failure. In other words, it is not possible to estimate the level of risk posed by the successful exploitation of a given vulnerability without considering the efficacy of the security controls that have been or are to be implemented to mitigate or eliminate the potential for such an exploitation; nor the threat's motivation, opportunity, and capabilities, which contribute to the likelihood of a successful attack; nor the impact to the system and organization should successful exploitation of a vulnerability occur. The following four steps—control analysis, threat likelihood determination, threat impact analysis, and risk determination are, in a practical sense, performed simultaneously or nearly simultaneously because they are so tightly linked to each other.

2.1.4.1. Control Analysis

As previously discussed, the analysis of controls in place to protect the system can be accomplished using a checklist or questionnaire, which is based on the security requirements for the system[5], also provides guidance on testing security controls. The results are used to strengthen the determination of the likelihood that a specific threat might successfully exploit a particular vulnerability.

2.1.4.2. Threat Likelihood Determination

Threat likelihood determination considers a threat source's motivation and capability to exploit a vulnerability, the nature of the vulnerability, the existence of security controls, and the effectiveness of mitigating security controls. Likelihood ratings are described in the qualitative terms of high, moderate, and low, and are used to describe how likely is a successful exploitation of a vulnerability by a given threat. For example, if a threat is highly motivated and sufficiently capable, and controls implemented to protect the vulnerability are ineffective, then it is highly likely that the attack would be successful. In this scenario, the appropriate likelihood rating would be high.

2.1.4.3. Threat Impact Analysis

Another factor used in determining the level of risk to a system is impact. A proper overall impact analysis considers the following factors: impact to the systems, data, and the organization's mission. Additionally, this analysis should also consider the criticality and sensitivity of the system and its data. FIPS 199 provides a consistent, focused process for categorizing a system's criticality and sensitivity for the three security domains of confidentiality, integrity, and availability. Using FIPS 199 to determine a security category and applying an assessment of the system's and organization's mission using tools such as mission-impact reports, asset criticality assessment reports, and business impact analyses results in a rating describing the estimated impact to the system and organization should a threat successfully exploit a vulnerability. While impact can be described using either a quantitative or qualitative approach, in the context of IT systems and data, impact is generally described in qualitative terms. As with the ratings used to describe likelihood, impact levels are described using the terms of high, moderate, and low[3].

2.1.4.4. Risk Determination

Once the ratings for threat likelihood and threat impact have been determined through appropriate analyses, the level of risk to the system and the organization can be derived by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact. Table 10-1 shows how to calculate an overall risk rating using inputs from the threat likelihood and impact categories using a 3X3 matrix. Depending on the requirements of the system and the granularity of risk assessment desired, 4x4 and 5x5 matrices may be used instead. A Very High risk level may require possible system shutdown or stopping all information system integration and testing effort.

Table 1
Risk Level Matrix

Threat Likelihood	*Impact* *Low (10)*	*Moderate (50)*	*High (100)*
High (1.0)	10 × 1.0 = 10	50 × 1.0 =50	100 × 1.0 = 100
Moderate (0.5)	10 × 0.5 = 5	50 × 0.5 = 25	100 × 0.5 = 50
Low (0.1)	10 × 0.1 = 1	50 × 0.1 = 5	100 × 0.1 = 10

Risk Scale: High(>50 to 100), Moderate (>10 to 50), Low (1 to 10).

Because the determination of risk ratings for impact and threat likelihood is largely subjective, it is best to assign each rating a numeric value for ease of calculation. The rationale for this justification can be explained in terms of the probability assigned for each threat likelihood level and a value assigned for each impact level.

Table 2 below describes the risk levels shown in the above matrix (Table 1). This risk scale, with its ratings of high, moderate, and low, represents the degree of risk to which an information system, facility, or procedure might be exposed if a given vulnerability were exploited. It also describes the type of action senior managers must take for each risk level.

Table 2
Risk Scale and Necessary Management Action

Risk Level	Risk Description and Necessary Management Action
High	If an observation or finding is evaluated as high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place at the earliest.
Moderate	If an observation is rated as moderate risk, corrective actions are needed and plan must be developed to incorporate these actions within a reasonable time.
Low	If an observation is evaluated as low risk, the system's authorizing official need to determine whether corrective actions are at all required, or decide to accept the risk.

2.1.5. Step 5 – Control Recommendations[5]

The goal of the control recommendations is to reduce the level of risk to the information system and its data to a level the organization deems acceptable. These recommendations are essential input for the risk mitigation process, during which the recommended procedural and technical security controls are evaluated,

prioritized, and implemented. This step is designed to help agencies identify and select controls appropriate to the organization's operations and mission that could mitigate or eliminate the risks identified in the preceding steps. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

- Effectiveness of recommended options;
- Legislations and regulation;
- Organizational policy;
- Operational impact; and
- Safety and reliability.

2.1.6. Results Documentation

The risk assessment report is the mechanism used to formally report the results of all risk assessment activities. The intended function of this report is to describe and document the risk posture of the system while it is operating in its stated environment (as described in the system characterization) and to provide organization managers with sufficient information so that they can make sound, risk-based decisions, such as resources that must be allocated to the risk mitigation phase. Lastly, the agency should ensure that the results of the risk assessment are appropriately reflected in the system's Plan of Action and Milestones (POA&M) and System Security Plan.

At the least, the risk assessment report should include the following:

- Scope of the assessment based on the system characterization;
- Methodology used to conduct the risk assessment;
- Individual observations resulting from conducting the risk assessment; and
- Estimation of the overall risk posture of the system.

2.2. Risk Mitigation

The second phase of the risk management process is risk mitigation. Because it is impractical, if not impossible, to eliminate all risk from a system, risk mitigation strives to prioritize, evaluate, and implement the appropriate risk-reducing controls suggested from the risk assessment process[5].

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 use the ***least-cost approach*** and implement the ***most appropriate controls*** to decrease mission risk to an acceptance level, with ***minimal adverse impact*** on the organization's resources and mission.

Fig 3: Risk Mitigation Strategy

System and organizational managers may use several options to reduce the risk to a system. These options are risk assumption; risk avoidance; risk limitation; risk planning, research, and acknowledgement; and risk transference.

Figure 3 illustrates a straightforward strategy that can be used to determine whether risk mitigation actions are necessary. Working from each risk identified and analyzed in the first process risk assessment managers must then decide whether the risk is acceptable or unacceptable and, subsequently, whether to implement additional controls or not to mitigate unacceptable risks. The first decision box in the figure applies to those threats involving intentional attacks. Natural and unintentional human errors are not considered in this decision-making scheme because there are no associated costs to consider, and so the strategy progresses to the next decision box.

Once the decision has been made on which risks are to be addressed in the risk mitigation process, a seven-step approach is used to guide the selection of security controls:

- Prioritize actions;
- Evaluate recommended control actions;
- Conduct cost-benefit analysis;
- Select controls;
- Assign responsibility;
- Develop a safeguard implementation plan; and
- Implement selected controls.

The process of selecting controls to mitigate identified risks to an acceptable level is based on the security categorization of the system[4]. The security categorization is used in two ways: (i) determines which minimum baseline security controls are selected from NIST SP 800-53, and (ii) aids in estimating the level of risk posed by a threat/vulnerability pair identified during the risk assessment[3]. System security controls selected are grouped into one of the three categories of management, operational, or technical controls, and are

either preventive or detective in nature. There are three points in an "attack cycle" where controls can be implemented. One can choose controls to (i) 'prevent' an attack from succeeding, (ii) 'detect and respond' to an attack, (iii) 'recover' from an attack. In practice, to prevent an attack is preferred.

For new systems, once the security controls for the system have been identified and refined and an initial risk assessment conducted, the selected controls must be implemented. For legacy systems, the security controls that are selected are verified. Organizations can leverage controls used among multiple systems by designating them as common controls where implementation, assessment, and monitoring is conducted at an organizational level or by areas of specific expertise). The system owner must understand who is responsible for implementing these controls and identify the risk that this extension of trust will generate.

Because it is impracticable to eliminate all risk, it is important to note that even after the controls have been selected and implemented, some degree of residual risk will remain. The remaining residual risk should be analyzed to ensure that it is at an acceptable level. For federal agencies, after the appropriate controls have been put in place for the identified risks, the authorizing official will sign a statement accepting any residual risk and either authorize the operation of the new information system or request continued processing of the existing information system.

2.3. Evaluation & Assessment

The final phase in the risk management process is evaluation & assessment. The art of risk management in today's dynamic and constantly changing information technology (IT) environments must be ongoing and continuously evolving. Systems are upgraded and expanded, components are improved, and architectures are constantly evolving.

The security control evaluation and assessment, which is conducted during the Security Certification Phase of a system's security certification and accreditation, provides input needed to finalize the risk assessment[6]. The results are used to provide the Authorizing Official with the essential information needed to make a credible, risk-based decision on whether to authorize the operation of the information system. Ideally, the risk assessment activities would be conducted at the same time the system is being certified and accredited.

Many of the risk management activities are conducted during a snapshot in time—a static representation of a dynamic environment. All the changes that occur to systems during normal, daily operations have the potential to adversely affect the security of the system in some fashion, and it is the goal of the risk management evaluation and assessment process to ensure that the system continues to operate in a safe and secure manner. This goal can be partially reached by implementing a strong configuration management program. In addition, to monitoring the security of an information system on a continuous basis, agencies must track findings from the security control assessment to ensure they are addressed appropriately and do not continue to pose or introduce new risks to the system.

The process of managing risk permeates the Systems Development Life Cycle (SDLC), beginning with the early stages of project inception through the retirement of the system and its data. From inception forward, agencies should consider the possible threats, vulnerabilities, and risks to the system so that they can better prepare it to operate in its intended environment, securely and effectively, and within a select risk threshold, as deemed acceptable by an agency senior official during the security certification and accreditation process.

REFERENCE

[1] National Institute of Standards and Technology Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories,* June 2004.

[2] ISO/IEC International Standard ISO/IEC 17799, *Information Technology – Code of Practice for Information Security Management* February 2001.

[3] National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

[4] Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

[5] National Institute of Standards and Technology Special Publication 800-53, Rev. 1, *Recommended Security Controls for Federal Information Systems*, February 2006.

[6] National Institute of Standards and Technology Special Publication 800-37, *Guide for Security Certification and Accreditation of Federal Information Systems*, May 2004.

[7] Computer Security Act, 1987.

[8] National Institute of Standards and Technology Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004.

[9] National Security Agency (UK), The NSA Security Manual.

[10] GSA Publication, *A Guide to Planning, Acquiring, and Managing Information Technology Systems, Version 1*, December 1998.

[11] Information System Security Association (USA), *Generally Accepted Information Security Principles, Version 3.0.*

[12] Julia Allen, *The CERT Guide to System and Network Security Practice,* Addison Wesley, Boston.

[13] Micky Krause and Harold Tripton, *Information Security Management Handbook*, Auerbach, Boca Raton, Fl.