Risk Management in Information Security System

Deepak Kumar
Department of Computer Science & Applications, Vaish College, Rohtak-124001, Haryana (INDIA)
indian_deepakkumar@yahoo.com

Abstract
In information security system there are always some cases which come up with some risks. To handle the risks there must be risk management in information security system. 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 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). Risk management tries to balance the project working by resolving the issues regarding the risks occur in the software development process.

Keyword: Risk management, SDLC, information security.

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.

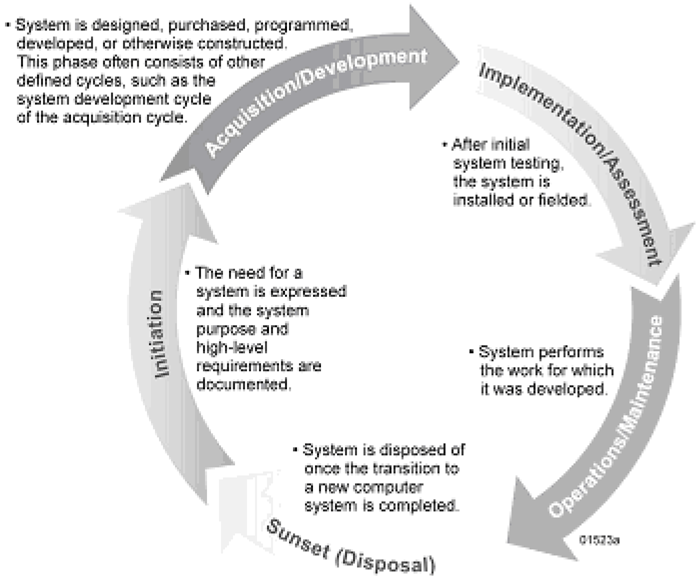
• System is designed, purchased, programmed, developed, or otherwise constructed. This phase often consists of other defined cycles, such as the system development cycle of the acquisition cycle.
Acquisition/Development
Implementation/Assessment
• After initial system testing, the system is installed or fielded.
Initiation
• The need for a system is expressed and the system purpose and high-level requirements are documented.
• System performs the work for which it was developed.
Operations/Maintenance
• System is disposed of once the transition to a new computer system is completed.
Sunset (Disposal)
01523a

Figure .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..

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

Risk = Threat x Vulnerability x 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 make 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]

1. Risk assessment – Risk assessment is the process of assess the vulnerability of the risk that how much potential the risk is.
2. 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.
3. 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.

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.

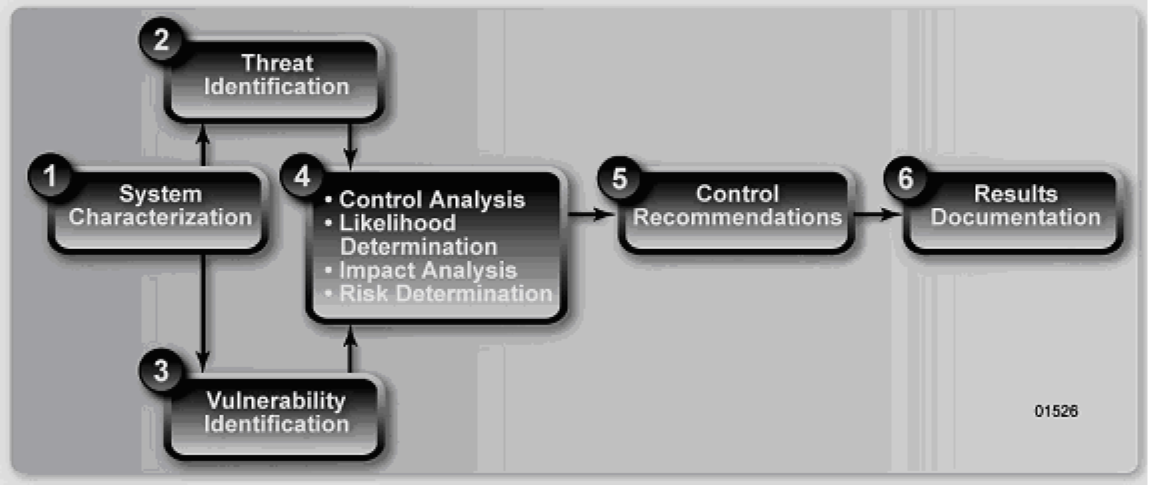

Figure 2. Risk Assessment Process

Risk Identification

Risk 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.

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.

Risk/ Threat Likelihood Determination

Threat likelihood determination considers a threat source's motivation and capability to exploit 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 potential, average, and minute are used to describe how likely a successful exploitation of vulnerability is 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.

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 potential, average and minute [3].

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

	Impact		
Threat Likelihood	**Minute (10)**	**Average (50)**	**Potential (100)**
Potential (1.0)	10 x 1.0 = 10	50 x 1.0 =50	100 x 1.0 = 100
Average (0.5)	10 x 0.5 = 5	50 x 0.5 = 25	100 x 0.5 = 50
Minute (0.1)	10 x 0.1 = 1	50 x 0.1 = 5	100 x 0.1 = 10

Risk Scale: Potential (>50 to 100), Average (>10 to 50), Minute (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 potential, average, and minute, 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**
Potential	If an observation or finding is evaluated as potential 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.
Average	If an observation is rated as average risk, corrective actions are needed and plan must be developed to incorporate these actions within a reasonable time.
Minute	If an observation is evaluated as minute risk, the system's authorizing official need to determine whether corrective actions are at all required, or decide to accept the risk.

Risk control suggestions [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.

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.

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].

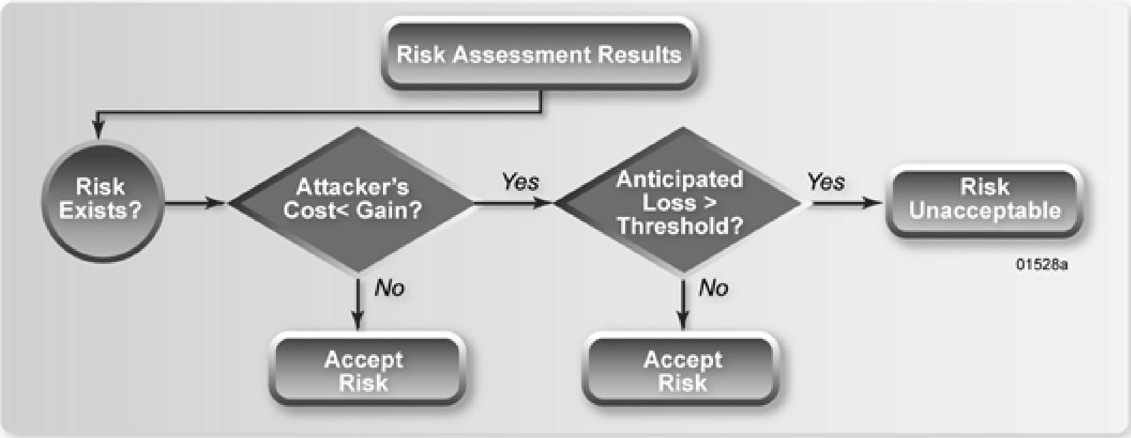

Figure 3. Risk Mitigation Strategy

Evaluation & Assessment

The final phase in the risk management process is evaluation & assessment. 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.

Conclusion

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.