International Research Journal of Management and Commerce
ISSN: (2348-9766)
Impact Factor- 5.564, Volume 5, Issue 3, March 2018
Website- www.aarf.asia, **Email** : editor@aarf.asia , editoraarf@gmail.com

RISK MANAGEMENT IN PURVIEW OF ONLINE TRANSACTION

Dr. Parag M. Joshi
Dhanwate National College
Nagpur (MS) India.

ABSTRACT

Every organization has a mission. In this digital era, as organizations use automated information technology (IT) systems1 to process their information for better support of their missions, risk management plays a critical role in protecting an organization's information assets, and therefore its mission, from IT-related risk.

An effective risk management process is an important component of a successful IT security program. The principal goal of an organization's risk management process should be to protect the organization and its ability to perform their mission, not just its IT assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization.

The objective of this paper is to analyse the organizational initiatives to accomplish its mission(s) (1) by better securing the IT systems that store, process, or transmit organizational information; (2) by enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget; and (3) by assisting management in authorizing (or accrediting) the IT systems3 on the basis of the supporting documentation resulting from the performance of risk management.

Keywords : Risk Management, online transaction, IT system

Introduction :

Risk management encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment. The risk assessment process, which includes identification and evaluation of risks and risk impacts, and recommendation of risk-reducing measures. Risk mitigation, which refers to prioritizing, implementing, and maintaining the appropriate risk-reducing measures recommended from the risk assessment process. The continual evaluation process and keys for implementing a successful risk management program. The 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 are the fundamental reasons organizations implement a risk management process for their IT systems. Effective risk management must be totally integrated into the SDLC. An IT system's

SDLC 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 phase.

Table 1 : Integration of Risk Management into the SDLC

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

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 ccomplishment.

  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.

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.

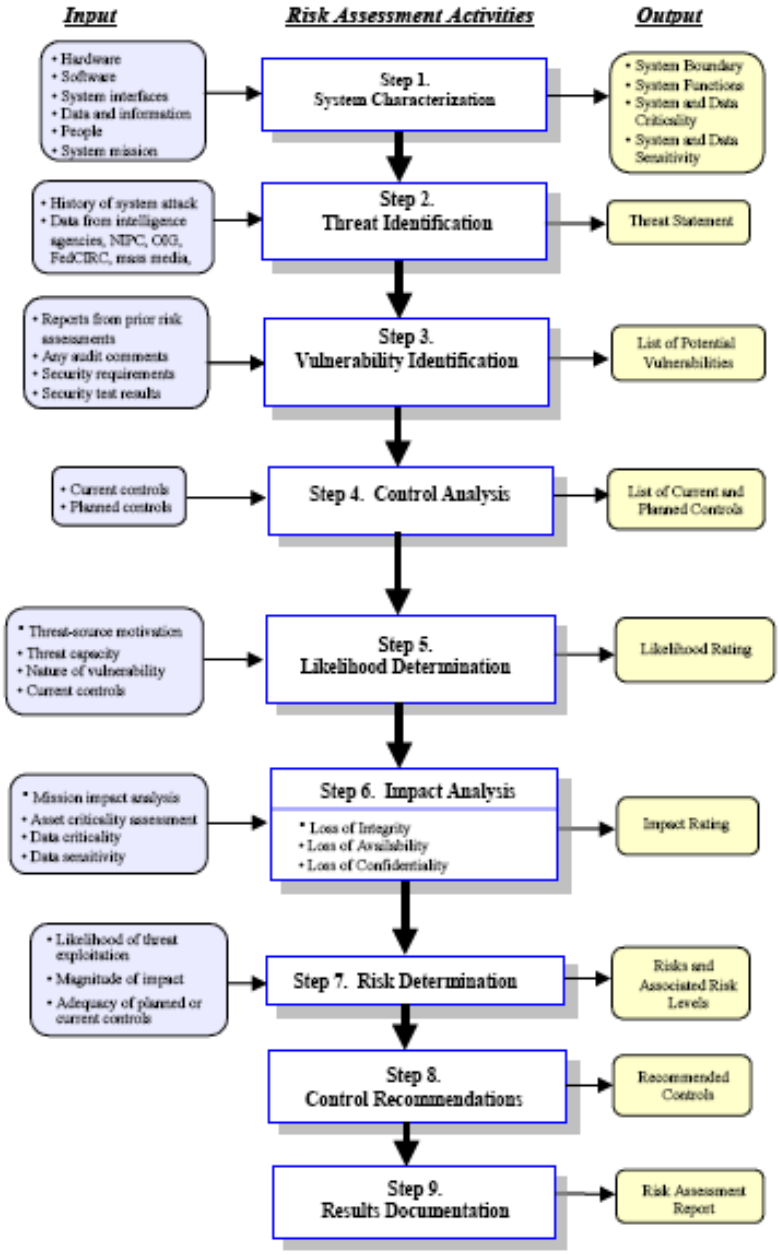
To determine the likelihood of a future adverse event, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT system.

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 in Sections 3.1 through 3.9

- Step 1: System Characterization
- Step 2: Threat Identification
- Step 3: Vulnerability Identification
- Step 4: Control Analysis
- Step 5: Likelihood Determination
- Step 6: Impact Analysis
- Step 7: Risk Determination
- Step 8: Control Recommendations
- Step 9 : Results Documentation

Steps 2, 3, 4, and 6 can be conducted in parallel after Step 1 has been completed. Following figure 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

STEP 2: THREAT IDENTIFICATION

A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. A vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present a risk when there is no vulnerability that can be exercised. In determining the likelihood of a threat, one must consider threat-sources, potential vulnerabilities, and existing controls.

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.

STEP 4: CONTROL ANALYSIS

The goal of this step is to analyze the controls that have been implemented, or are planned for implementation, by the organization to minimize or eliminate the likelihood (or probability) of a threat's exercising a system vulnerability.

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment (Step 5 below), the implementation of current or planned controls must be considered. For example, a vulnerability (e.g., system or procedural weakness) is not likely to be exercised or the likelihood is low if there is a low level of threat-source interest or capability or if there are effective security controls that can eliminate, or reduce the magnitude of, harm.

STEP 5: LIKELIHOOD DETERMINATION

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the following governing factors must be considered:

- Threat-source motivation and capability
- Nature of the vulnerability

- Existence and effectiveness of current controls.

The likelihood that a potential vulnerability could be exercised by a given threat-source can be described as high, medium, or low. Following Table describes these three likelihood levels.

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

STEP 6: IMPACT ANALYSIS

The next major step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of a vulnerability. Before beginning the impact analysis, it is necessary to obtain the following necessary information:

- 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.

This information can be obtained from existing organizational documentation, such as the mission impact analysis report or asset criticality assessment report. A mission impact analysis (also known as business impact analysis for some organizations) prioritizes the impact levels associated with the compromise of an organization's information assets based on a qualitative or quantitative assessment of the sensitivity and criticality of those assets. An asset criticality assessment identifies and prioritizes the sensitive and critical organization information assets (e.g., hardware, software, systems, services, and related technology assets) that support the organization's critical missions.

STEP 7: RISK DETERMINATION

The purpose of this step is to assess the level of risk to the IT system. The determination of risk for a particular threat/vulnerability pair can be expressed as a function of

- The likelihood of a given threat-source's attempting to exercise a given vulnerability

- The magnitude of the impact should a threat-source successfully exercise the vulnerability
- The adequacy of planned or existing security controls for reducing or eliminating risk.

To measure risk, a risk scale and a risk-level matrix must be developed.

STEP 8: CONTROL RECOMMENDATIONS

During this step of the process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization's operations, are provided. The goal of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

- Effectiveness of recommended options (e.g., system compatibility)
- Legislation and regulation
- Organizational policy
- Operational impact
- Safety and reliability.

The control recommendations are the results of the risk assessment process and provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented

STEP 9: RESULTS DOCUMENTATION

Once the risk assessment has been completed (threat-sources and vulnerabilities identified, risks assessed, and recommended controls provided), the results should be documented in an official report or briefing.

A risk assessment report is a management report that helps senior management, the mission owners, make decisions on policy, procedural, budget, and system operational and management changes. Unlike an audit or investigation report, which looks for wrongdoing, a risk assessment report should not be presented in an accusatory manner but as a systematic and analytical approach to assessing risk so that senior management will understand the risks and allocate resources to reduce and correct potential losses.

RISK MITIGATION

Risk mitigation, the second process of risk management, involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process.

Because the elimination of all risk is usually impractical or close to impossible, it is the responsibility of senior management and functional and business managers to use the ***least-cost approach*** and implement the ***most appropriate controls*** to decrease mission risk to an acceptable level, with ***minimal adverse impact*** on the organization's resources and mission.

RISK MITIGATION OPTIONS

Risk mitigation is a systematic methodology used by senior management to reduce mission risk. Risk mitigation can be achieved through any of the following risk mitigation options:

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

The goals and mission of an organization should be considered in selecting any of these risk mitigation options. It may not be practical to address all identified risks, so priority should be given to the threat and vulnerability pairs that have the potential to cause significant mission impact or harm. Also, in safeguarding an organization's mission and its IT systems, because of each organization's unique environment and objectives, the option used to mitigate the risk and

the methods used to implement controls may vary. The "best of breed" approach is to use appropriate technologies from among the various vendor security products, along with the appropriate risk mitigation option and non-technical, administrative measures.

EVALUATION AND ASSESSMENT

In most organizations, the network itself will continually be expanded and updated, its components changed, and its software applications replaced or updated with newer versions. In addition, personnel changes will occur and security policies are likely to change over time.

These changes mean that new risks will surface and risks previously mitigated may again become a concern. Thus, the risk management process is ongoing and evolving.

The good practice and need for an ongoing risk evaluation and assessment and the factors that will lead to a successful risk management program.

GOOD SECURITY PRACTICE

The risk assessment process is usually repeated at least every 3 years for various agencies, as mandated by Circular A-130. However, risk management should be conducted and integrated in the SDLC for IT 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.

There should be a specific schedule for assessing and mitigating mission risks, but the periodically performed process should also be flexible enough to allow changes where warranted, such as major changes to the IT system and processing environment due to changes resulting from policies and new technologies.

KEYS FOR SUCCESS

A successful risk management program will rely on (1) senior management's commitment; (2) the full support and participation of the IT team (see Section 2.3); (3) the competence of the risk assessment team, which must have the expertise to apply the risk assessment methodology to a specific site and system, identify mission risks, and provide cost-effective safeguards that meet the needs of the organization; (4) the awareness and cooperation of members of the user community, who must follow procedures and comply with the implemented controls to

safeguard the mission of their organization; and (5) an ongoing evaluation and assessment of the IT-related mission risks.

CONCLUSION :

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. 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 real world 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.

References :

- Ashby, W.R., *An Introduction to Cybernetics*, Chapman and Hall, London, 1956.
- Anderson, R., and T. Moore. 2006. "The Economics of Information Security." Science 314, no. 5799 (October 27): 610-3.
- Bakos, J.Y., "Dependent Variables for the Study of Firm and Industry-Level Impacts of Information Technology," in J.I. DeGross and C.H. Kriebel (Eds.), *Proceedings of the Eighth International Conference on Information Systems*, Pittsburgh, Pennsylvania, (December 6-8, 1987), pp. 10- 21.
- Bakos, J.Y. & Treacy, M.E., "Information Technology and Corporate Strategy: A Research Perspective," *MIS Quarterly*, 10, 2, (June 1986).
- Benjamin, R. & Blunt, J.,"Critical IT Issues: The Next Ten Years," *Sloan Management Review*, (Summer 1992), 7- 19.
- Benjamin, R. & Levinson, E., "A Framework for Managing IT- Enabled Change," Sloan Management Review, (Summer 1993), 23- 33.

- Federal Financial Institutions Examination Council. 2004. Retail Payments System: IT Examination Handbook. March. Available at .
- Sullivan, R. J. 2007. “Risk Management and Nonbank Participation in the U.S. Retail Payments System.” Federal Reserve Bank of Kansas City Economic Review 92, no. 2 (second quarter): 5-40.
- www.bis.org
- www.firstatlanticcommerce.com/banks/risk-reporting/
- https://www.phe.gov
- www.djaa.com
- www.researchgate.net