Assessment Risk Management Information Technology Systems

Marzieh zare nazari

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.
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 paper 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.
Index Terms— Information Technology, Risk Management, Risk Assessment.

1 INTRODUCTION

A management information system (MIS) is a system or process that provides the information necessary to manage an organization effectively. MIS and the information it generates are generally considered essential components of prudent and reasonable business decisions.
The importance of maintaining a consistent approach to the development, use, and review of MIS systems within the institution must be an ongoing concern of both bank management and OCC examiners. MIS should have a clearly defined framework of guidelines, policies or practices, standards, and procedures for the organization. These should be followed throughout the institution in the development, maintenance, and use of all MIS.
MIS is viewed and used at many levels by management. It should be supportive of the institution's longer term strategic goals and objectives. To the other extreme it is also those everyday financial accounting systems that
are used to ensure basic control is maintained over financial recordkeeping activities. Financial accounting systems and subsystems are just one type of institutional MIS. Financial accounting systems are an important functional element or part of the total MIS structure. However, they are more narrowly focused on the internal balancing of an institution's books to the general ledger and other financial accounting subsystems. For example, accrual adjustments, reconciling and correcting entries used to reconcile the financial systems to the general ledger are not always immediately entered into other MIS systems.[9]

Accordingly, although MIS and accounting reconcilement totals for related listings and activities should be similar, they may not necessarily balance.
An institution's MIS should be designed to achieve the following goals:
• Enhance communication among employees.
• Deliver complex material throughout the institution.
• Provide an objective system for recording and aggregating information.
Management Information Systems 2 Comptroller's Handbook
• Reduce expenses related to labor-intensive manual activities.
• Support the organization's strategic goals and direction.
Because MIS supplies decision makers with facts, it supports and enhances the overall decision making process. MIS also enhances job performance throughout an institution. At the most senior levels, it provides the data and information to help the board and management make strategic decisions. At other levels, MIS provides the means through which the institution's activities are monitored and information is distributed to management, employees, and customers.
Effective MIS should ensure the appropriate presentation formats and time frames required by operations and senior management are met. MIS can be maintained and developed by either manual or automated systems or a combination of both. It should always be sufficient to meet an institution's unique business goals and objectives. The effective deliveries of an institution's products and services are supported by the MIS. These systems should be accessible and useable at all appropriate levels of the organization.[8]

Marzieh zare nazari, Graduate and faculty member of the Department of computer, Anar Branch, Islamic Azad University, Anar, Iran, PH:+989132933945,
E_mail: marzieh.nazari@gmail.com

2 Risks Associated With MIS

Risk reflects the potential, the likelihood, or the expectation of events that could adversely affect earnings or capital. Management uses MIS to help in the assessment of risk within an institution. Management decisions based upon ineffective, inaccurate, or incomplete MIS may increase risk in a number of areas such as credit quality, liquidity, market/pricing, interest rate, or foreign currency. A flawed MIS causes operational risks and can adversely affect an organization's monitoring of its fiduciary, consumer, fair lending, Bank Secrecy Act, or other compliance-related activities.

Since management requires information to assess and monitor performance at all levels of the organization, MIS risk can extend to all levels of the operations. Additionally, poorly programmed or non-secure systems in which data can be manipulated and/or systems requiring ongoing repairs can easily disrupt routine work flow and can lead to incorrect decisions or impaired planning.[2]

3 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. This paper 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.[11]

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.

3.1 key Roles Of Risk Management

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 require-

ments 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.[7]

-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.[1]

3.2 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).

4 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.

This section describes risk mitigation options, the risk mitigation strategy , an approach for control implementation, control categories, the cost-benefit analysis used to justify the implementation of the recommended controls, and residual risk .[5]

4.1 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 nontechnical, administrative measures.[3]

4.2 Risk Mitigation Strategy

Senior management, the mission owners, knowing the potential risks and recommended controls, may ask, "When and under what circumstances should I take action? When shall I implement these controls to mitigate the risk and protect our organization?"

This strategy is further articulated in the following rules of thumb, which provide guidance on actions to mitigate risks from intentional human threats:

-When vulnerability (or flaw, weakness) exists ?

implement assurance techniques to reduce the likelihood of a vulnerability's being exercised.

-When a vulnerability can be exercised ?

apply layered protections, architectural designs, and administrative controls to minimize the risk of or prevent this occur-

rence.

-When the attacker's cost is less than the potential gain ? apply protections to decrease an attacker's motivation by increasing the attacker's cost (e.g., use of system controls such as limiting what a system user can access and do can significantly reduce an attacker's gain).

-When loss is too great → apply design principles, architectural designs, and technical and nontechnical protections to limit the extent of the attack, thereby reducing the potential for loss.

The strategy outlined above, with the exception of the third list item ("When the attacker's cost is less than the potential gain"), also applies to the mitigation of risks arising from environmental.[10]

5 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.

This section emphasizes the good practice and need for an ongoing risk evaluation and assessment and the factors that will lead to a successful risk management program.[4]

5.1 Good Security Practice

The risk assessment process is usually repeated at least every 3 years for federal agencies, as mandated by OMB 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.[6]

6 Conclusion

Organizations can analyze the extent of the risk reduction generated by the new or enhanced controls in terms of the reduced threat likelihood or impact, the two parameters that define the mitigated level of risk to the organizational mission.A successful risk management program will rely on (1) senior management's commitment; (2) the full support and participation of the IT team; (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.[12]

References

[1] ELECTRONIC SOURCE: Appel, W.M.G., Enterprise Architecture - An In-Depth Study, 2009, EACommunity, http://www.eacommunity.com/articles/openarticle.asp?ID=1840, accessed in 2012.

[2] ELECTRONIC SOURCE: Malhotra, Y., Enterprise Architecture - An Overview, 1996, Brint Institute, http://www.brint.com/papers/enterarch.htm, accessed in 2011.

[3] ELECTRONIC SOURCE: West, D., K. Bittner, and E. Glenn, Ingredients for Building Effective Enterprise Architectures, 2012, The Rational Edge, http://www-106.ibm.com/developerworks/rational/library/content/RationalEdge/nov02/EnterpriseArchitectures_TheRationalEdge_Nov2002.pdf, accessed in 2012.

[4] ELECTRONIC SOURCE: Malveau, R., Bridging the Gap: Business and Software Architecture, Part 2, 2009, Cutter Consortium, www.cutter.com/research/2004/edge040203.html, accessed in 2010.

[5] ELECTRONIC SOURCE: Malhotra, Y., Enterprise Architecture - An Overview, 2012, Brint Institute, http://www.brint.com/papers/enterarch.htm, accessed in 2004

[6] JOURNAL ARTICLE: Zachman, J., The Framework for Enterprise Architecture and the Search for the owner`s view of business rules. Database Newsletter, 2011. 27(1).

[7] JOURNAL ARTICLE: Nezlek, G.S., H.K. Jain, and D.L. Nazareth, An integrated approach to enterprise computing architectures. Communications of the ACM, 2010 42(11): p. 82-90.

[8] CONFERENCE PROCEEDINGS: Nightingale, D. and D.H. Rhodes. Enterprise Systems Architecting: Emerging Art and Science within Engineering Systems. in MIT Engineering Systems Symposium. 2009.

[9] CONFERENCE PROCEEDINGS: Van Belle, J.P. Moving Towards Generic Enterprise Information Models: From Paciolo to Cyc. in Australian Conference on Information Systems. 2012.

[10] CONFERENCE PROCEEDINGS: Leidich, J.C. Use of Enterprise Architecture to Manage Technical Complexity at the U.S. Bureau of the Census. in Joint ECE/Eurostat/OECD meeting on the management of statistical informatin systems. 2013.

[11] CHAPTER IN A BOOK: Steen, M.W.A., et al., Service-Oriented Enterprise Architecture, in Service-Oriented Software System Engineering: Challenges and Practices, Z. Stojanivic and A. Dananayake, Editors. 2009.