ISSN: 2321-7782 (Online)
Volume 3, Issue 4, April 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Information Security Risk Management for Enterprises

Manoj[1]
Deptt. of CSE
Sat Kabir Institute of Technology & Management (SKITM)
Bahadurgarh, Haryana, India

Shabnam Sangwan[2]
Deptt. of CSE
Sat Kabir Institute of Technology & Management (SKITM)
Bahadurgarh, Haryana, India

Abstract: Information security risk management is becoming essential for establishing a safe environment in enterprises for their day to day operations & activities. This research paper is concerned with presenting a comprehensive Information Security Risk Management Framework that enables the effective establishment of the target safe environment.

As managing information risk becomes an increasingly important business concern, one of the challenges for organizations is to understand when and how to integrate Information Risk Management framework into the organization. This paper combines Industry standards, guidelines and best practices associated to information security risk management.

Keywords: Risk Assessment, Risk Identification, Risk Analysis, Risk Evaluation, Risk Treatment, Residual Risk

I. INTRODUCTION

Every business as we know it cannot exist without information and the technology that delivers that information. It is this dependency on information and information technology that has raised the need to manage risk associated with information.

Regulatory compliance (i.e. ISO 27001:2013 Information Security Control 6.1.2, 6.1.3 & HIPAA - Health Insurance Portability and Accountability Act for healthcare customers only) for managing information properly, information risk begins to reach into all layers of company governance. In fact when we consider that nearly every business process and activity is enabled by integrated information and shared information resources, it is very plausible to say that information risk intensifies all other areas of risk within a business. Each company's Risk Management system is different because their risks are different, their operations and Organizations are unique, and their corporate culture is unique.

In order to manage this new area of risk, a common definition of what information risk is must be adopted. "Risk, the possibility of damage or loss, is described mostly in dependencies of threat and vulnerability, or impact and probability."

In this International Standard such as ISO 31000, NIST, the expressions "risk management" and "managing risk" are both used. In general terms, "risk management" refers to the architecture (principles, framework and process) for managing risks effectively, while "managing risk" refers to applying that architecture to particular risks.

When implemented and maintained, the risk management enables an organization to, for example:

» Increase the likelihood of achieving objectives;

» Encourage proactive management;

» Be aware of the need to identify and treat risk throughout the organization;

» Improve the identification of opportunities and threats;

» Comply with relevant legal and regulatory requirements and international norms;

» improve mandatory and voluntary reporting;

» Improve governance;

» Improve stakeholder confidence and trust;

» Improve organizational resilience.

II. Literature Review

The literature review for the research facilitates the analysis of literature materials. Examples of these include different frameworks, standards, policies, procedures etc. Risk Management is one of the major components of Information Security Domain.

Although it is widely known, a wide range of approaches for Risk Management are found in the relevant literature [ISO 27005], International Standards Organization/International Electro technical Commission ISO/IEC 27005:2011 [1] provides guidelines for information security risk assessment, treatment, acceptance, communication, monitoring and review in the enterprise. [NIST Guidelines], National Institute of Standards and Technology [6] came up with thorough Guide for Applying the Risk Management Framework to Federal Information Systems. NIST is working with public and private sector entities to establish specific mappings and relationships between the security standards and guidelines developed by NIST and the International Organization for Standardization and (ISO/IEC) 27001:2005/2013 (new standard), Information Security Management System (ISMS) and ENISA Regulation [5] Risk Management/ Risk Assessment in European regulation, international guidelines and codes of practice. Introduction to Information System Risk Management – SANS [4] Institute Study. The common goal of these methods is to prioritize and estimate the risk value and to suggest the most suitable mitigation plan to eliminate or minimize that risk to an acceptable level

These all guidelines and standard generally accepted by Information Security experts or enterprises. Risk Management is a recurrent activity that deals with the analysis, planning, implementation, control and monitoring of implemented measurements and the enforced security policy. On the contrary, Risk Assessment (as part of Risk Management) is executed at discrete time points (e.g. once a year, on demand, etc.) and – until the performance of the next assessment - provides a temporary view of assessed risks in entire Risk Management process. All big enterprises implemented Information Security Risk Management, and establish an Information Security Risk Management Frameworks, Procedures and Guidelines. This could reduce threat and vulnerabilities associated within enterprise or organization, the risk to the organization or to individuals associated with the operation of an information system.

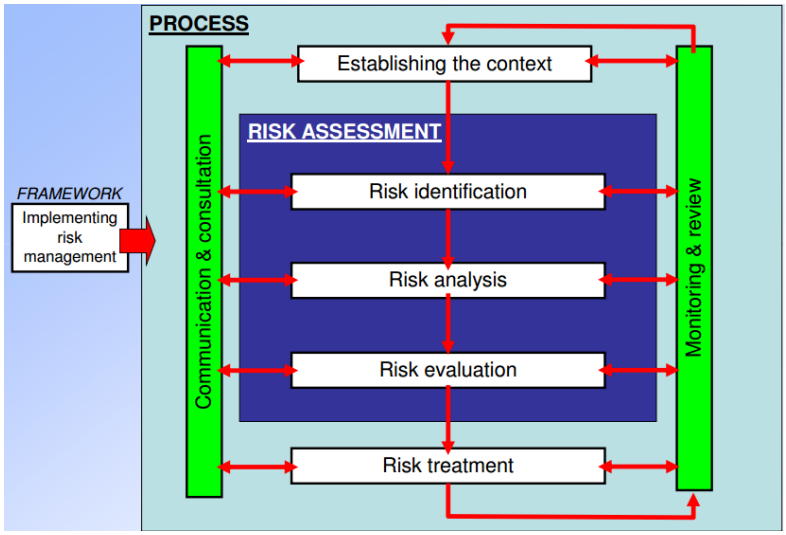
III. Proposed And Scope

The purpose of this risk management program is to conduct appropriate activities to assess and mitigate risks associated with information assets/ resources. The paper will identify areas of risk considered as sensitive and requiring monitoring on an on-going basis. Stakeholders will properly document this monitoring, in the form of risk assessment activities.

The scope includes relating the project to business objectives, and defining the boundaries of the project in multiple dimensions including approach, deliverables, milestones, and budget ETC. The “scope” of the framework is based on the domains of strategy, technology, organization, people, and environment with different levels of details, associated with each domain.

IV. Risk Management Framework

According to ISO 31000 Standard, a risk management framework is a set of components that support and sustain risk management throughout an organization. There are two types of components: foundations and organizational arrangements. Foundations include your risk management policy, objectives, mandate, and commitment. And organizational arrangements include the plans, relationships, accountabilities, resources, processes, and activities you use to manage your organization’s risk.



Risk Management Process Diagram

A. How Is Risk Assessed?

Risk is assessed by identifying **threats and vulnerabilities**, then determining the likelihood and impact for each risk. It's easy, right? Unfortunately, risk assessment is a complex undertaking, usually based on imperfect information. There are many methodologies aimed at allowing risk assessment to be repeatable and give consistent results.

a) **Threat:** The potential for a threat source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

b) **Vulnerability:** 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

Risk Assessment: Risk Assessment is a process that is, in turn, made up of three processes: ***risk identification, risk analysis, and risk evaluation.***

1. Risk Identification:

» Process of finding, recognizing and describing risks

» Comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives.

» Identify the risks associated with not pursuing an opportunity

» A risk that is not identified at this stage will not be included in further analysis

» Identification should include risks whether or not their source is under the control of the organization

2. Risk Analysis:

» Process to comprehend the nature of risk and to determine the level of risk

» "Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur."

» Provides the basis for risk evaluation and decisions about risk treatment

» Risk analysis includes risk estimation

3. **Risk Evaluation:**

» The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation

» Decisions should take account of the wider context of the risk and include consideration of the tolerance of the risks borne by parties other than the organization that benefit from the risk

» Decisions should be made in accordance with legal, regulatory and other requirements

» In some circumstances, the risk evaluation can lead to a decision to undertake further analysis

» The risk evaluation can also lead to a decision not to treat the risk in any way other than maintaining existing controls

B. Risk Treatment

Risk treatment involves selecting one or more options for modifying risks, and implementing those options. Risk treatment options are not necessarily mutually exclusive. The options can include the following:

1. **Transfer:**

» Sharing the risk with another party or parties.

» Transference is the process of allowing another party to accept the risk on your behalf.

2. **Avoid:**

» Avoidance is the practice of removing the vulnerable aspect of the system or even the system itself.

» Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk

» Removing the risk source

3. **Mitigate:**

» Mitigation involves fixing the flaw or providing some type of compensatory control to reduce the likelihood or impact associated with the flaw.

» Changing the likelihood

» Changing the consequences (impact)

4. **Accept:**

» Acceptance is the practice of simply allowing the system to operate with a known risk. Many low risks are simply accepted. Risks that have an extremely high cost to mitigate are also often accepted. Beware of high risks being accepted by management.

» Taking or increasing the risk in order to pursue an opportunity

Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived, with regard to legal, regulatory, and other requirements such as social responsibility and the protection of the natural environment. A number of treatment options can be considered and applied either individually or in combination.

Risk treatment itself can introduce risks. A significant risk can be the failure or ineffectiveness of the risk treatment measures. Monitoring needs to be an integral part of the risk treatment plan to give assurance that the measures remain effective.

C. What is Residual Risk?

Residual risk is the risk left over after you've implemented a risk treatment option. It's the risk remaining after you've reduced the risk, removed the source of the risk, modified the consequences, changed the probabilities, transferred the risk, or retained the risk.

Residual risk is a threat that remains after an organization has implemented security controls to comply with legal requirements.

There are four basic ways of dealing with risk: reduce it, avoid it, accept it or transfer it. Since residual risk is unknown, many organizations choose to either accept residual risk or transfer it.

D. Monitoring & Review

An integral part of the risk management process involving regular checking or surveillance

» Ensure controls are effective & efficient

» Detect change in external or internal context

» Analysis, lessons learned, continuous improvement

» Identify emerging risks

Employees can pose security threats to your enterprise IT infrastructure through mobile devices such as smart phones and laptops, as well as the various networks and applications with which their unsecured devices are liable to interact. Enterprise Information Security Executives, IT administrators, network administrators, and enterprise security workers and consultants should be aware of these security risks.

E. Following are the ways where employees pose a security risk for your organizations:

» **Laptop** - Employees are taking laptops everywhere, especially as they get lighter, making them more vulnerable to loss or theft.

» The **unauthorized or accidental** release of classified, personal, or sensitive information by an individual or employee.

» **P2P** – Applications such as Skype and instant messaging create security holes that can let Trojans and other spyware onto your network, particularly if employees are allowed to share those infected files

» **USB Flash Drives** – USB (such as pen drives) may carry viruses

» **Unauthorized Software Updates** - Allowing employees to download patches or upgrades before your networks are ready can render user PCs and the network itself vulnerable to hacks and other security attacks.

» **Social Networks** - Face book and MySpace in particular are unsecured and invite employees to share critical information while wasting time, while add-on applications available through those sites could hide malware and spyware, posing additional security threats

» **Collaboration Tools & Hosted Software** - Collaboration tools such as SharePoint, wikis and even e-mail distribution systems are great in theory but security risks in practice, unless administrators actively monitor the distribution and usage of user names and passwords. Not taking these security measures leaves the systems open to people who should not have access.

» **Alteration of Software** - An intentional modification, insertion, deletion of operating system or application system programs, whether by an authorized user or not, which compromises the confidentiality, availability, or integrity of

data, programs, system, or resources controlled by the system. This includes malicious code, such as logic bombs, Trojan horses, trapdoors, and viruses.

» **Smart Phones** - Allowing employees to bring nonstandard - issue smart phones and PDAs into the workplace, which will not integrated as BYOD

» **Wi-Fi** - Logging onto unsecured wireless networks at home, the local Starbucks or on the road leaves data at risk unless employees are careful to log onto networks through a VPN or take other security measures.

» **Web Mail** - Employees sending sensitive work files to their unaudited personal Web addresses are vulnerable to having their accounts hacked and critical company data stolen

Other well known Organization level Risks:

» **Application's malware** poses high risks towards software codes

» **Other Technical Vulnerabilities** related to **Network Architecture and Server Management**

» Lack of **Vulnerability scanning, antivirus** and **patch management**

» System Configuration Error – An accidental configuration error during the initial installation or upgrade of hardware, software, communication equipment or operational environment.

» **Subcontractors, or suppliers** or other business associates who are not under the direct control of the business

» **Acts of Nature** - All types of natural occurrences (e.g., earthquakes, hurricanes, tornadoes) that may damage or affect the system/application. Any of these potential threats could lead to a partial or total outage, thus affecting availability

F. Communicating Risks and Risk Management Strategies

Risk must also be communicated. Once risk is understood, risks and risk management strategies must be clearly communicated to organizational management in terms easily understandable to organizational management.

With a **quantitative risk assessment methodology**, risk management decisions are typically based on comparing the costs of the risk against the costs of risk management strategy. A return on investment (ROI) analysis is a powerful tool to include in the risk assessment report. This is a tool commonly used in business to justify taking or not taking a certain action.

With a **qualitative risk assessment methodology**, the task is somewhat more difficult. While the cost of the strategies is usually well known, the cost of not implementing the strategies is not, which is why a qualitative and not a quantitative risk assessment was performed. Including a management-friendly description of the impact and likelihood with each risk and risk management strategy is extremely effective. Another effective strategic is showing the residual risk that would be effective after the risk management strategy was enacted.

G. How we can derive Qualitative Technology Risks :

Level	Likelihood Definitions
High (1.0)	The threat source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Moderate (.5)	The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low (.1)	The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Impact Analysis: The adverse impact of a security event in terms of loss or degradation of any, or a combination of any, of the following three security goals, resulting from successful exploitation of vulnerability:

» Loss of Confidentiality – Impact of unauthorized disclosure of confidential information (ex. Privacy Act). Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

» Loss of Integrity – Impact if system or data integrity is compromised by intentional or accidental changes to the data or system.

» Loss of Availability – Impact to system functionality and operational effectiveness should systems be unavailable to end users.

Magnitude of Impact	Impact Definitions
High (100)	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Moderate (50)	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm or impeded an organization's mission, reputation, or interest; or (3) may result in human injury.
Low (10)	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources; (2) may noticeably affect an organization's mission, reputation, or interest.

Risk Level Determination: These levels represent the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised:

» 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.

Magnitude of Impact	Risk Level Definitions
High (>50-100)	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 as soon as possible.
Moderate (>10-50)	Corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low (1-10)	The system's Authorizing Official must determine whether corrective actions are still required or decide to accept the risk.

H. Risk Calculation Worksheet

The following NIST SP 800-30 calculation worksheet provides instructions for determining the overall risk level for this report. History of past occurrences can help determine the threat likelihood level and impact level can take into account, financial impact, employee safety, and many other factors.

Threat Likelihood	Impact		
	Low (10)	**Medium (50)**	**High (100)**
High (1.0)	Low 10 x 1.0 = 10	Medium 50 x 1.0 = 50	High 100 x 1.0 = 100
Medium (0.5)	Low 10 x 0.5 = 5	Medium 50 x 0.5 = 25	High 100 x 1.0 = 50
Low (0.1)	Low 10 x 0.1 = 1	Medium 50 x 0.1 = 5	High 100 x 1.0 = 10
Risk Scale : High (>50 to 100); Medium (>10 to 50); Low (1 to 10)8			

1. Risk Scale and Necessary Actions

The following Risk Scale and Necessary Actions table presents actions that NIST SP 800-30 recommends senior management (the mission owners) must take for each risk level. Your Organization should determine if this, or another methodology, will be used.

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a 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 as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's Designated Approving Authority (DAA) must determine whether corrective actions are still required or decide to accept the risk.

V. CONCLUSION

We have defined Risk Management Framework/ Process during the research that could be an approach to implement an Information Security Risk Management. In summary, successful and effective risk management is the basis of successful and effective Information Security controls and compliance to various regulatory requirements. Due to the reality of limited resources and nearly unlimited threats, a reasonable decision must be made concerning the allocation of resources to protect systems. Risk management practices allow the organization to protect information and business process commensurate with their value. To ensure the maximum value of risk management, it must be consistent and repeatable, while focusing on measurable reductions in risk. Establishing and utilizing an effective, high quality risk management process and basing the information security activities of the organization on this process will lead to an effective information security program in the organization. We can implement effective risk management framework in companies so that all threats and vulnerabilities are identified and risks are highlighted and mitigate n stipulated time.

VI. FUTURE SCOPE

Though the framework and process steps for effective risk management implantation has been demonstrated by use of different strategies, but there have been some limitations in the research work carried out in this thesis. One of the limitations, in the proposed framework is purely based on Quantitative methodology. This requires tool intervention who can classify all security risks, threats and vulnerabilities associated within Organization. In future this research effort can be put on to a dedicated Risk Management Quantitative Methodology via Tool (OCTAVE, FRAP, COBRA and Risk Watch etc.). Hence, there is a lot of future scope of the research work to be carried out in this vital area of great significance to mankind.

ACKNOWLEDGMENT

I would like to thanks my worthy guide Ms. Shabnam Sangwan, who suggested me to work and research Information Security Risk Management. Her recommendations, innovative ideas and constructive criticism contributed to make the success of this report. Her numerous suggestions, comments, and advice have made this entire paper possible.

References

1. http://www.iso27001security.com/html/27005.html - ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management (second edition)
2. ISO 31000 Standard for Risk Management – Principles and Guidelines
3. Principles of Information Security By Michael Whitman, Herbert Mattord
4. http://www.sans.org/reading-room/whitepapers/auditing/introduction-information-system-risk-management-1204
5. ENISA Risk Management Regulation (Risk Management / Risk Assessment in European regulation, international guidelines and codes of practice)
6. http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf
7. http://www.cert.org/octave/osig.html - Information security risk assessment and management

8. http://www.isaca.org/knowledge-center/risk-it-it-risk-management/pages/default.aspx
9. https://privacyassociation.org/news/a/web-conference-bringing-risk-management-from-theory-to-practice

AUTHOR(S) PROFILE

Manoj, received the B.E degree in Computer Science & Engineering from Bhagwan Mahavir Institute of Technology & Management (BMIET), Sonepat affiliated to Maharshi Dayanand University, Rohtak (Haryana) and pursuing M.Tech (2013 to 2015 batch) from Sat Kabir Institute of Technology and Management (SKITM), Bahadurgarh affiliated to Maharshi Dayanand University, Rohtak (Haryana). Currently I am doing research on Information & Data Security – A Serious concern to IT Organizations. I am thankful to Management and staff of college who is supporting me during my entire research/ Thesis work.

Shabnam Sangwan, received the B.Tech degree in Computer Science & Engineering from Maharaja Surajmal Institute of Technology (MSIT), affiliated to Guru Gobind Singh Indraprastha University, New Delhi and M.Tech degree in Computer Science & Engineering from PDM college of Engineering, affiliated to Maharshi Dayanand University, Rohtak (Haryana) in 2011 and 2013 batch respectively. She is presently working in Sat Kabir Institute of Technology and Management (SKITM), Bahadurgarh, Haryana, India and had associated with PDM polytechnic, Bahadurgarh earlier to this.

