Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 2, Issue 1, pp: (82-88), Month: January - April 2015, Available at: www.noveltyjournals.com

Risk Management in Information System of Organisation: A Conceptual Framework

[1]Mrs. Neeti Mathur, [2]Mr. Himanshu Mathur, [3]Miss Trapti Pandya

[1]Research Scholar, Department of Accounting Shramjeevi College, J.R.N.V. University, Udaipur, India
[2]Financial Analyst, HSBC Global Solutions, Kolkata, India
[3]Research Scholar, Department of Banking and Financial Management, Shramjeevi College, J.R.N.V. University, Udaipur, India

1. INTRODUCTION

Information system plays a key role for survival and growth of any organisation. To maintain effective and efficient information system is not an easy task for IT Professionals. The basic task of information security is to support the mission of the organization and maintain its existence.

All organizations are exposed to unknown risk which harms the organization. There are several risk to which the Information System is exposed, like fire, virus, hackers etc. These risks should be properly identified and manage in order to support the organization. We can say risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. Managing risk is difficult due to changing technologies, limited resources, threats and vulnerabilities .Due to all these problems it is very difficult to completely mitigating all risks. Therefore, to maintain good information system is challenge for IT Professionals. So, they must have appropriate cost effective techniques to assist them in mitigating risks to a reasonable level. It is needed to manage this risk to maintain confidentiality, integrity or availability of information system.

2. REVIEW OF LITERATURE

David Kim and Michael Solomon (Learning Information Systems Security and Assurance 2010), provides a comprehensive overview of the essential concepts of Information System. There is a discussion of the new risks, threats, and vulnerabilities associated with the transformation to a digital world, including a look at how business, government, and individuals operate today.

Hanson, David (Risk Management Information Systems, 2005) , explains that Managing Risk in Information Systems provides a unique, in-depth look at how to manage and reduce IT associated risks. This includes Risk, Response, and Recovery Domain in addition to providing a thorough overview of risk management and its implications on IT infrastructures and compliance. The book provide the fundamentals of risk management, strategies and approaches for mitigating risk, and the anatomy of how to create a plan that reduces risk.

Duden, David and Geaglone, Peter in there article For Risk Managers – Enterprise Risk Systems ,(Risk & Insurance Technology Magazine,2006)discuss the organisation related risk which are face by the management and provide the action plan to mitigate and control the risk.

Michael Stewart, in their study on Network Security, Firewalls, and VPNs provides a unique, in-depth look at the major business challenges and threats that are introduced when an organizations network is connected to the public Internet.

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 2, Issue 1, pp: (82-88), Month: January - April 2015, Available at: www.noveltyjournals.com

3. RESEARCH OBJECTIVES

1) To understand the risk and risk related terms, along with acquire a conceptual knowledge of threats in information system.

2) To explain a systematic approach for risk management and control in Information system which provide basic guideline to help organisations to manage risk.

3) To identify the gaps emerged in information system of organisation.

4. RESEARCH METHODOLOGY

a) The research for this subject is done as an exploratory research. This Exploratory research provides conceptual framework for risk management in the information system of the organisation.

b) The data is collected is secondary in nature which is collected from Books, Journals, Internet, News Papers etc.

5. LIMITATIONS OF STUDY

The research provide conceptual framework for risk management it is not specific for any organisation .It just provide basic guideline for the risk management.

6. SOME IMPORTANT TERMS RELATED TO RISK

Threats: Threats is an action or event which may cause harm to organisation. There are several problem arises due to threat they are disclosure of confidential information, data destruction, business continuity problems.

Vulnerabilities: It is a weakness in the safeguard or security of the system due to which information system exposed to various threats. 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.

Exposure: It is an impact of risk in an immediate and long term.

Likelihood: Determining likelihood is fairly straightforward. It is the probability that a threat caused by a threat-source will occur against vulnerability. In order to ensure that risk assessments are consistent, it is an excellent idea to utilize a standard definition of likelihood on all risk assessments.

Low	0-25% chance of successful exercise of threat during a one-year period
Medium	26-75% chance of successful exercise of threat during a one-year period
High	76-100% chance of successful exercise of threat during a one-year period

Figure 2 – Sample Likelihood Definitions

Attack: It is a malicious actions which may compromise the integrity and confidentially and other desired features of information system.

Residual Risk: This is the risk remains even after all the security majors and controls to prevent the risk are implemented. It is difficult to overcome or mitigate a100% impact of any risk. Therefore, management of organisation needs to decide the acceptance level of a risk. Acceptance level of a risk is a residual risk.

7. THREATS TO INFORMATION SYSTEM

1) Risk to the computerised environment:

The following are some important threats to computerised environment.

a) Power Loss: Power failure can disrupt the entire computing environment and its working.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 2, Issue 1, pp: (82-88), Month: January - April 2015, Available at: www.noveltyjournals.com

b) Communication Failure: Failure of communication devices may result in disruption of working of computers based system.

c) Fire: It may occur due to short circuit in electronic wire and due to other explosive products. Fire can provide huge loss to the organisation.

d) Misuse by employee: Dissatisfied employee can harm an organisation by intentionally destroying or disclosing sensitive information.

e) Technological Failure: It cause immense loss to the organisation.

f) Malicious code: Means malicious programs such as viruses and destructive programs like torjan hourse, worms, logic bomb etc. These programs may affect organisation and computer network.

g) Natural disaster: Such as flood, lightening, earthquake, tsunami etc. can provide a big damage to information system.

h) Theft and destruction of computing resources: It result in economic and reputation loss of organisation.

2) Risk due to Cyber Crime: Cybercrime is a "electronic offences " and it becoming more and more evident due to increasing use of computer networks and internet, and frauds conducted .

a) Fraud: It is an unlawful activity which is primarily related to unauthorised and unlawful use of ATM and Debit cards.

b) Sabotage: It is an intentional damage of web pages and malicious alteration of data.

c) Computer Virus: They are destructive programs which can affect other programs in computer and sometimes result in big losses to organisation, in terms of loss of productivity and continuity of losses.

d) Embezzlement: It is unlawful misappropriation of money by a person to whom the responsibility of electronic fund transfer is entrusted. Generally employee of the organisations are engage in it.

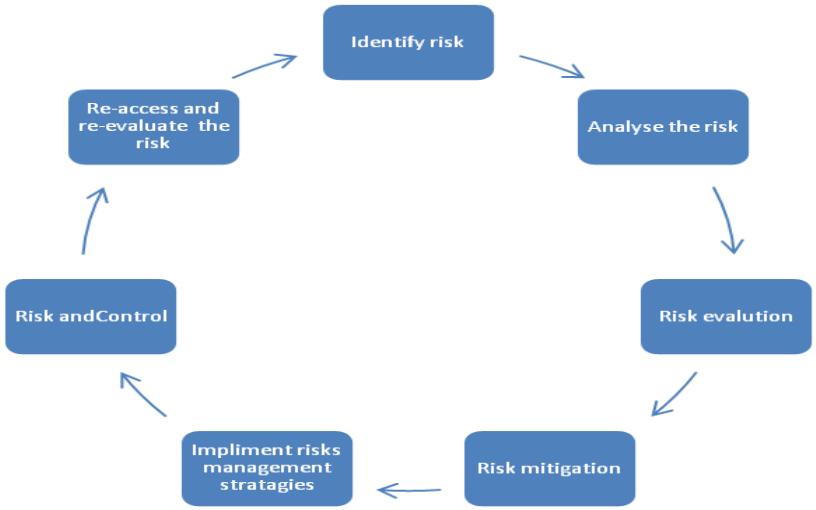
These are several threats or risk associated with the organisations to overcome these threats the process of risk management, which is also known as risk management cycle is developed.

8. RISK MANAGEMENT CYCLE

Risk management is a systematic process of series of steps taken to manage and control the risks for organisation or controls the risks for an IT system.

Risk management includes procedures and steps for identifying, analysing, evaluating, treating, monitoring and communicating risk. Risk management is iterative process as it used repetitively, so it is also known as risk management cycle.

The risk management cycle involve following steps;



International Journal of Novel Research in Computer Science and Software Engineering
Vol. 2, Issue 1, pp: (82-88), Month: January - April 2015, Available at: www.noveltyjournals.com

1. Risk Identification:

For this purpose risk factors which are associated internal (means from within the organisation) and external (from outside the organisation) like assets and services of organisation and other legal financial, reputation and operational implications.

Information system is exposed to many direct and indirect risks. These risks are primarily having emerged due to frequent technological changes in information systems. These technological changes create gaps between protection applied and protection required for information systems.

2. Risk analysis and evaluation techniques:

After identification of risk, it should be further analysed and evaluated to take the decision whether to accept the risk or mitigate the risks. The decision to accept or mitigate the risks depends upon the impact of risk on organisation if risk materializes. Here acceptances means do not apply any controls for risks management and mitigate means apply control to manage the risks.

The risk mitigations are measures or controls implemented to avoid or reduce the probability of occurrence of risks. Excessive risk and excessive control are not useful aspects; therefore, there should be a balance between these two.

Outcome of excessive risks	**Outcome of excessive controls**
Loss of assets	Increased bureaucracy
Poor business decisions	Reduced productivity
Non-compliance	Increased complexity
Increased regulations	Increased processing cycle time
Increased frauds	Increase of activities having no values

The purpose of risk analysis and evaluation is to analyze the impact of risk by:

1. Identifying the probability of threats.

2. Exposure i.e the damage or loss to assets when threats occur.

Risk: Probability of Threat x Exposure (loss) of Threat.

Risk analysis and evaluation flow chart

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 2, Issue 1, pp: (82-88), Month: January - April 2015, Available at: www.noveltyjournals.com

9. IMPORTANT TECHNIQUES FOR RISK ANALYSIS AND EVALUTION

1. Judgement and intuition: In this technique the auditor use its judgement and intuition for risk analysis and evaluation. It is based on its personal and professional experience and its understanding of system and environment. It is required for auditor to continuously update his knowledge for risk management.

2. Delphi Techniques: In this technique a panel of expert is appointed and each expert provides his opinion in written and independent manner. In this technique ,each expert lists out possible threats to the system and then estimates the expected probability of threats occurrence and possible losses to arrive at risks estimates, These estimates are analysed and risks having above target estimates are accepted. All the experts opinions are combined and a median range is drawn to finalise the risks to the system.

3. Quantitative Technique: In this technique a possible risk impact by multiplying exposure of risk with probability of risk occurrence. The technique helps organisations to select the cost effective solution for risk management because the selected solution's cost should be lower than the possible risk impact.

4. Qualitative Technique: It is a more like a judgement approach but involves analysis of more elements that judgement technique. In this approach, probability data is not required and only estimated potential loss is used. Based on the analysis of possible threats, vulnerabilities for threats and applied controls, auditor provides the potential risks to the system under analysis.

Two quantitative parameters are used for risk ranking.

1. Probability of occurrence, means

Probability	weight
High	10
Medium	5
Low	1

2. Exposure of threat is second parameter.

Impact	**Weight**	**Remark**
No impact	0	no interruption to working
Noticeable impact	1	interruption can be unto8 hours
Bigger damage	2	interruption can be more than 8 to 48 hours.
Major damage	3	interruption can be for many days

Based on above techniques, weighted risk factor for every risk or threat is calculated and accordingly ranking is done for all the factors.

3. Risk assessment:

As the potential threat is identified, the system is reviewed to find out weaknesses that can be exploited by threats and likelihood of those threats which are discuss earlier in this paper.

4. Mitigation:

Mitigation is the most commonly considered risk management strategy. Mitigation involves fixing the flaw or providing some type of compensatory control to reduce the likelihood or impact associated with the flaw. There are several measures, include administrative and technical controls, which can be used to mitigate risks.

a) Transference:

Transference is the process of allowing another party to accept the risk on your behalf. This is not widely done for IT systems, but everyone does it all the time in their personal lives. Car, health and life insurance are all ways to transfer risk. In these cases, risk is transferred from the individual to a pool of insurance holders, including the insurance company

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 2, Issue 1, pp: (82-88), Month: January - April 2015, Available at: www.noveltyjournals.com

b) Acceptance

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.

c) Avoidance

Avoidance is the practice of removing the vulnerable aspect of the system or even the system itself. For instance, during a risk assessment, a website was uncovered that let vendors view their invoices, using a vendor ID embedded in the HTML file name as the identification and no authentication or authorization per vendor. In this case, the risk was avoided by removing the vulnerable web pages.

5. Implementation of risk management:

The first step in implementing risk management strategies is to get management to approve the Plan of action and milestone. Afterwards, the various individuals and teams report upon their progress and communicate to management.

A Plan of Action & Milestones (POAM) should be part of the risk assessment report presented to management. Basically POAM is a tool to communicate to management on the proposed and actual completion of the implementation of the risk management strategies.

6. Risk and control:

The risk mitigations are measures or controls implemented to avoid or reduce the probability of occurrence of risks. Excessive risk and excessive control are not useful aspects; therefore ,there should be a balance between these two.

Outcome of excessive risks	Outcome of excessive controls
Loss of assets	Increased bureaucracy
Poor business decisions	Reduced productivity
Non-compliance	Increased complexity
Increased regulations	Increased processing cycle time
Increased frauds	Increase of activities having no values

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 controls is to reduce the level of risk to the IT system and its data to an acceptable level. To determine which one is appropriate for a specific organization, a cost-benefit analysis is done.

7. Re-evaluation and re-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. Due to this reason re-evaluation and re- assessment will lead to a successful risk management program. 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.

10. GAPS OBSERVED IN INFORMATION SYSTEM OF ORGANISATION

These gaps developed between protections applied and protection required for information systems. The main gaps are:

1. Frequent technological changs create difference between old and new technology and due to this reason the old risk management system become in sufficient in managing risk in new system this gap create risk in organisation information system.
2. Wide use of internet exposes the organisation information system for virus, vandalism, intrusion, hacking etc.
3. Widespread use of new technologies without proper risk management.

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 2, Issue 1, pp: (82-88), Month: January - April 2015, Available at: www.noveltyjournals.com

4. Decentralisation of management and control cerate leakage of corporate confidential and price sensitive information and cause huge harm to organisation.
5. Some external factors such as legal and regulatory requirement like right of information allow hacking, misuse of information by the employee and theft of important information.

11. CONCLUSIONS AND RECOMMENDATIONS

1. The effective risk management needs an good understanding of the threats associated external and internal to the organisation.
2. Proper frame work to identify, analyse, evaluate, mitigate control the risk should be made.
3. As the resources are limited and unlimited threats are present, a reasonablendecision must be made concerning the allocation of resources to protect systems.
4. Risk management practices allow the organization to protect information and business process commensurate with their value. To effective risk management, it must be consistent and repeatable, while focusing on measurable reductions in risk.
5. There are several tools available to manage an efficient risk management system ,a cost benefit analysis should be done before implementation of risk management system.

REFERENCES

[1] Chadwick, William, Global Trends in the Information Technology Outsourcing Services Market, USITC, Industry and Technology Review (ITTR), Nov. 2003.

[2] Geetika Sharma, “Challenges of the Indian IT Service Industry”, May 18,2009

[3] Horton, Thomas. “Managing Information Security Risks”(March 2012)-page 18-55

[4] Siddharth A. Pai and Deepak Khosla, Has the US Slowdown Hit IT Sector? The Economic Times, 25 April 2008.

[5] “IT Disaster”, E-Business, April 2009,pg13-34

[6] National Institute of Standards and Technology Special Publication 800-30,

[7] Risk Management Guide for Information Technology Systems (May 2011) – page 12

[8] Risk Management Guide for Information Technology Systems (July 2011) – page 8

[9] Siddharth A. Pai and Deepak Khosla, Has the US Slowdown Hit IT Sector? The Economic Times, 25 April 2008,pg23-26

[10] Wipro Council for Industry Research http://www.wipro.com/resource-center/wipro-council-forindustry-research/pdf/recession_ and_its_impact_on_it_industry.pdf

Websites:

[11] www.nasscom.org

[12] www.ezinearticles.com

[13] www.google.co.in

[14] www.smallbusinessnotes.com

[15] www.scholargoogle.com

[16] www.scribd.com