Enhancing Information Security Risk Management for Organizations

Subir Kochar [#1], Sachin Goyal [*2], Ratish Agarwal [*], Mahesh Pawar [*]
[#]*Cyber law& Information Security, NLIU, Bhopal, Madhya Pradesh, India*
[*]*Information Technology, RGPV, Bhopal, Madhya Pradesh, India*

Abstract - *Risk is defined as the uncertainty of results which can be either positive opportunity or a threat for the organization. The research will start from introduction of risks, impact of risk, Risk Factors, Type of Risks. Risk management which is a critical area is then focused for assessing, optimizing risks. A major part in risk management is risk assessment and analysis which derives data for decision making. Risk management is summarized including the different phases of it including risk identification, assessment and mitigation. A glimpse of desirable characteristics of an ideal risk management is also mentioned. After that problem like no identification procedure for critical controls, problem with management of dynamic risks and selection of existing methodology are discussed. The research will go through the comparative framework of existing methodologies for easing selection and also Talks about ISO 27005 and COBIT framework for overcoming the problems.*

Keywords - *Risk Management, Risk Assessment, Risk Identification, Risk Mitigation, COBIT*

I. Introduction

In the early 90's the growth of Internet started and with that availability of information. In the beginning, there were less dependency on the internet and less complex systems with considerable risks were in play which made them easier to secure unlike today. Now, Information is the most important asset for the organization with varying levels of commercial value and sensitivity. The fortunes of most organizations are tied with the information they possess and sophistication with which they are able to manage it. In modern days there is a lot of dependency on use of IT which creates risks. The technologies and methods used by an organization create a number of risks and threats to the valuable information. Information needs to be protected from the risks of being stolen, misused, unauthorized access, modification, unavailability etc. There are many types of risks that emerge within an organization like physical, environmental, financial, security etc which may cause loss to an organization.

Risk is defined as the uncertainty of results which can be either positive opportunity or a threat for the organization. Information security is hardly a new concept. The need to protect valuable information is as old as mankind. Information is a primary asset for organization so protection of it is also of prime importance. Risk management of information becomes an important aspect in the organization's security strategies. Risk need to be assessed considering the events that can happen and impact of that events on organizations if they occur. Increasing e-commerce industry, outsourcing of IT assets etc have been the factor for increasing concern on managing risks. A risk strategy should be made with a business approach and cover all aspects for a complete picture of risk.

Risk management is a policy driven process where many strategies for protecting organization from risk are applied and decisions regarding certain acceptable risks are taken. The strategy may include different solutions like reduction, mitigation, reallocation of risk. The identification, measuring and management of organizational risk for improving management decisions and overall performance are done through risk management. The main aim of risk management is to flourish organizations business with assets protection. Many organizations follow different frameworks for information security risk management but International standard ISO/IEC 27005 is the authentic and common standard. ISO 27005 is based upon the information security management system (ISMS) framework for achieving effective management of risks.

Risk management includes Risk identification, Risk assessment, Risk analysis, Risk mitigation. Identification of risk is the initial step in building risk profile and evaluating risk. Risk assessment is process of studying, analyzing set of outcomes and likelihoods in an organization for identifying and understanding risk. Organizations used different risk management methodologies from last few years which were continuously improving. Most of these risk management methodologies, while providing a structured and systematic process for risk management, either lack specific guidance on which risk assessment methods to use or provide for a weak approach. The use of new methodologies has overcome certain old problems but still needs more developments. There is a no clear guidance on how risk assessment should be done in a structured manner.

Risk a possibility of an event is defined and importance of information security in information risk management is discussed by Bob blakley et al [1]. Elena Ramona Stroie et al [2] elaborates basic concepts of risk management, approach followed and the risk management process. Organization’s risk management process to protect the organization and its ability to perform their mission given by NIST [3].The stepping stone for risk management is efficient risk assessment achieved with a risk assessment process like in risk assessment guide by GAO [4]. Venkata Kiran Maram et al [5] discussed countermeasures to be taken by assessing the potential vulnerabilities. Difficulty in finding appropriate risk management method is reduced by a comparative framework by W.G Borman et al [6]. Key differences and commonalities between the various Risk Assessment methodologies are discussed by Dan Ionita [7]. Armaghan Behnia et al [8] compared and clarify different activities, inputs, and outputs required by each model of information security risk assessment and analysis. Also, choices of risk assessment methods that allow an organization for information security risk are given by K.V.D.Kiran et al [9]. Traditional information technology (IT) security risk assessment approaches based on an analysis of events, probabilities are given in Stefan Taubenberger et al [10]. The dynamic nature of emergent hazards which requires new techniques and analytical frameworks are studied by Denis Smith et al [11]. Cobit addresses need for management and control of information and technology [12]. OCTAVE implementation for small and medium companies is described by Pyka Marek [13].

II. PROBLEMS

Existing risk assessment methods provides a framework for efficient risk management but have certain issues during implementation by organizations. There are some gaps that arise in most of the risk assessment approaches and its implementation. Risk assessment mostly use qualitative approach thus depending on the decision makers. These lack certain parameters due to which certain desirable characteristics will not be met.

A. *Critical Controls*

In an organization it is very expensive to test each and every control so prioritization of controls is done by the responsible person according to organization’s critical assets. There exists no formal procedure for identifying these controls and it depends on the judgement of assessors. Some of the methodologies are qualitative so these do not consider risk appetite and cost so sufficient data is not given to decision makers and configuration of critical controls become difficult.

B. *Changing threats*

The threats in the environment are constantly changing and new risks are emerging each day which is creating problems for organization. The risk management process used by organizations is static and capable of dealing with specific risks. Most of the risk management methods do not effectively assess changing risks only a glimpse of it. The process needs to be dynamic in nature to adapt under changing circumstances.

C. *Selection of Risk assessment method*

In information security there is a wide range of existing risk assessment methods and models. Some of them use qualitative approach and other quantitative approach. There are generic method for most kinds of risk and also methods for specific risk. These methods can be complex, time consuming, may not cover some of organization’s objectives so selection of the best assessment method for organization is difficult and there is no procedure for it.

III. RISK MANAGEMENT

Risk management is a process consisting on:

- Identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives.
- Risk assessment by setting the probability and impact of its production.
- Identify possible countermeasures and deciding which one could be applied, based on the value of information resource to the organization. [2]

Risk management has become a necessary step for an organization every time a decision needs to be done for any event or improvement. The process should include all the necessary steps for efficient working of organization to achieve objectives. It is a continuous improvement process with its implementation reaching to highest management level. Risk management can be done using two approaches reactive and proactive approach. The reactive approach depends on incidents; it is a response for the already occurred security risks. In proactive approach, measures are taken from the beginning and do not wait for incidents to occur.

Risk management is a continuous process which contains some permanent steps that needs to be followed. The compulsory steps include identification of business requirements for designing system then implementing control measures and procedures. After implementing, effectiveness of controls must be checked by monitoring, reassessing. At last, improvements and updating necessary for enhancing system must be done.

Risk management process starts with establishing of context which includes identification of objective and scope of project. It also includes identification of relevant stakeholders, internal/ external factors. The primary part of risk management process is Risk assessment. Risk assessment is used as a tool for determining the extent of threats and risk by organization. The steps followed in risk assessment includes risk identification, risk analysis and risk evaluation.

Risk identification depends on the way risk has been defined. Identification of critical assets by analyzing the company's activities, processes, information systems and other important factors that support organization are done in this phase. It identifies some potential threat sources and affects of it on the systems. Confidentiality and Integrity of the data are compromised by human and non-human threats. It also identifies some of the weaknesses and defects that may be exploited by threats involved. Vulnerabilities can be identified according to the nature of IT systems and developments. No backups, unauthorized changes, inadequate training etc are some vulnerability that can be exploited by fires, earthquakes, technical malfunction etc.

After the identification of threats and vulnerabilities the controls, causes and consequences are being analyzed. The existing controls are in place or not for mitigating the risk impact and controls are sufficient or not. Assessing the likelihood of vulnerability that can be exploited and scaling it into high, medium or low. Assessing the consequences of a potential threat and the intensity of it during the events occurred.

Next step is Risk evaluation in which risk is acceptable or unacceptable is decided. If the organization can tolerate the risk associated or treatment is unavailable, costly then it is accepted. Acceptable and tolerable risks need to be monitored and treated as soon as possible for increasing organization's security.

After the risk assessment phase, all the possible options for risk treatment are identified. Risk treatment is about modification of risk within an organization. Treatment includes decision regarding necessary treatment according to the risk, designing preferred treatment option (which will reduce likelihood), evaluating treatment options, Documentation of risk treatment plan used.

IV. DESIRABLE CHARACTERISTICS FOR RISK MANAGEMENT

Risk management should follow an approach which must include certain desirable characteristics for efficient risk management and counter the loopholes in existing methodologies. Some of the characteristics are:

- To manage risk to an acceptable level based on Organization's risk appetite.
- It should be a continuous process. Risk management should be done throughout a software lifecycle and not at specific points only.
- It should be in-line with the organization's objectives and work to fulfil those objectives.
- It must be consistent with the results produced and should not be affected by factors that may affect it.
- It must be adaptive as there are frequent changes in the organization like change in threats, vulnerabilities with changing effects.
- It must also be scalable as the increased complexity of systems should not affect other risk management activities.

V. ENHANCING RISK MANAGEMENT

A comparative study of risk management methodologies for the organization to select the appropriate method is given below. This can be used as a framework for comparing exiting methodologies.

TABLE I
COMPARATIVE FRAMEWORK FOR RISK METHODOLOGIES

Methods	Approach	Cost	Compliance	Skill required	Tools
OCTAVE	Qualitative	Low	No	Standard	Yes
CRAMM	Qualitative	High	ISO/IEC 17799	Specialist	No
ISRAM	Quantitative	Low	ISO/IEC 17799 ISO/IEC 13335	Standard	Yes
CORAS	Qualitative	Low	ISO/IEC 31000 ISO/IEC 17799	Standard	Yes
CORA	Quantitative	High	No	Standard	Yes
IS	Quantitative	Low	No	Standard	No

ISO/IEC 27005 has given a set of guidelines for information security risk management within context of information security management system (ISMS). It provides an iterative approach for conducting risk assessment with increasing accuracy and creates a balance for identifying controls but still miss certain key steps in identification of controls. The continuous iterations in ISO 27005 makes it applicable for changing environments as it is a repetitive scenario so any change can be identified and dealt accordingly. In this process after risk assessment process is completed a decision point is given for calculating the satisfactory result of the assessment process conducted and if it is not satisfactory the whole process is repeated. Similarly after risk treatment also decision point is there for satisfactory treatment. In these if the risk and threats changes or increases resulting in unsatisfactory risk assessment then in the second iteration it can be identified and treated to secure from it.

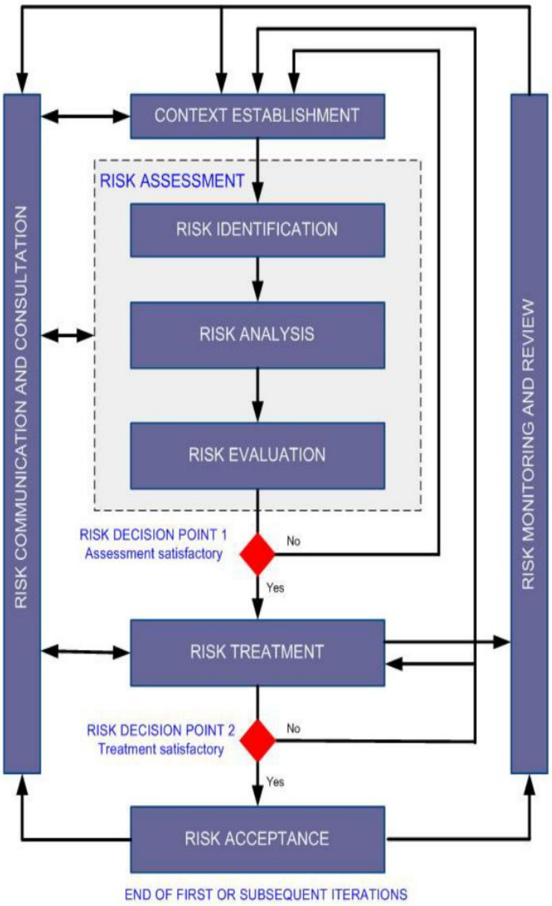

Fig. 1: ISO/IEC 27005 Risk management process

COBIT (Control objectives for IT and Available Technology) 4.1 provides a process model under its four domains including Plan and organize, Acquire and implement, Deliver and support, Monitor and evaluate. In these 4 domains it has identified 34 main IT processes and for all these COBIT has defined control objectives. It contains control objectives, assurance guidelines, performance and outcome metrics, critical success factors and maturity models which give a granular view about organization, its current status and areas of improvement. It gives objectives according to which critical controls can be prioritized and completely analyzed data for decision making is provided. Critical controls are selected by using this framework and not just by random pickings.

VI. CONCLUSION

Risk management is a continuous process for protecting organization from risks and vulnerabilities. Effective risk management depends upon perfect assessment of risk and its affects. The problems mentioned above are faced by organizations so the use of comparative Framework of methodologies can solve the selection problem. Changing nature of threats and Identification of critical controls can be taken care with the use of COBIT framework and aligning it with ISO/IEC 27005 standards. The merging of technologies should be done so that features of both can be utilized for effective risk management and risk analysis. The future of risk management is bright as more and more research is going on to meet the requirements of the changing environment and continuous improvement is done.

REFERENCES

[1] Bob Blakley, Ellen McDermott, Dan Geer, Information Security is Information Risk Management.

[2] Elena Ramona Stroie, Alina Cristina RUSU, Security Risk Management - Approaches and Methodology, 2011

[3] Gary Stoneburner, Alice Goguen and Alexis Feringa, Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology Special Publication 800-30, 2002

[4] Information Security Risk Assessment Practices of Leading Organizations, US General accounting office, GAO, 1999

[5] Venkata Kiran Maram, A Study of Risk Management of an Information System by Assessing Threat, Vulnerability and Countermeasure, International Journal of Advanced Research in Computer Science and Software Engineering

[6] W.G. Borman, L. Labuschagne, A comparative framework for evaluating information security risk management methods, South Africa, 2004

[7] Dan Ionita, Current Established Risk Assessment Methodologies and Tools, 2013

[8] Armaghan Behnia et al, A Survey of Information Security Risk Analysis Methods, Smart Computing Review, vol. 2, 2012

[9] K.V.D.Kiran et al, Performance And Analysis of Risk Assessment Methodologies In Information Security, International Journal of Computer Trends and Technology (IJCTT), Vol. 4 Issue 10, 2013

[10] Stefan Taubenberger et al, Problem Analysis of Traditional IT-Security Risk Assessment Methods – An Experience Report from the Insurance and Auditing domain.

[11] Denis Smith & Moira Fischbacher, The changing nature of risk and risk management: The challenge of borders, uncertainty and resilience, Editorial Review, 2009

[12] Chitra Baggar, Richa Sinha, Identification And Analysis Of Risks For Cloud Computing In IAAS, PAAS And

SAAS, International Journal of Computer Organization Trends Volume 3 Issue 9, 2013

[13] John W. Lainhart, Journal of information systems, Vol. 14, 2000, Cobit: A methodology for managing and controlling information technology risks and vulnerabilities.

[14] Pyka Marek, Januszkiewicz Paulina, The OCTAVE methodology as a risk analysis tool for business resources, Proceedings of the International Multi conference on Computer Science and Information Technology, 2006

[15] Bob Blakley, Ellen McDermott, Dan Geer, Information Security is Information Risk Management

[16] Ketil Stølen, Folker den Braber, Theo Dimitrakos, Rune Fredriksen, Bjørn Axel Gran, Siv-Hilde Houmb, Mass Soldal Lund, Yannis C. Stamatiou and Jan Øyvind Aagedal, Model-based risk assessment – the CORAS approach

[17] Guide for Conducting Risk Assessments, Computer Security Division and Information Technology Laboratory, NIST Special Publication 800-30, 2013

[18] Artur Rot, IT Risk Assessment: Quantitative and Qualitative Approach, Proceedings of the World Congress on Engineering and Computer Science, 2008

[19] Michel Crouhy, Dan Galai and Robert Mark, The Essentials of Risk Management, McGraw-Hill publication, 2009

[20] ISO/IEC 27001: 2011, Information technology – Security techniques – Information security risk management, BSI, 2011