International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 5, Issue 3 (May-Jun 2017), PP. 158-161

APPRAISE OF RISK MANAGEMENT APPROACHES IN IT PROJECTS

Suruchi Shukla[1], Dr Anshu Srivastava[2],
[1]Research Scholar, Shri Venkateshwara University, Gajraula,
[2]Research Supervisor, Shri Venkateshwara University, Gajraula,
UP, India

***Abstract*— By definition, project risks are indecisive events or conditions that, if occurs has a harmful effect on project's objectives. Contrasting, positive uncertain events are called opportunities. More, risk analysis aims its practices to be tailored to the project and congruent with the organizational culture, processes and assets. Risks are lopsidedly significant, that's why it is very important to filter and prioritize risks for further attention. Risk analysis is essential for successful project management and aims to recognize and prioritize risks in advance of their occurrence, and provide action-oriented information to project managers. This work will focus on the risk analysis of distributed software projects. In developing a common frame of reference concerning management of distributed software projects, the conceptual foundations of previous research are analyzed. Additionally, practice and research-related challenges for managing distributed software projects are presented. Addressing these challenges is the crucial area of concern for this study**

***Index Terms*— Risk, Probability, APM , Risk cost, DRiMaP models.**

I. A DEFINITION AND INTRODUCTION TO RISK

Practitioner's definitions for concepts are important because they are often used extensively by industry and by research. The APM is a professional body that publishes a well-researched Body of Knowledge (2011), and this defines risk as "the potential of an action or event to impact on the achievement of objectives." James Ward, an independent consultant specialising in systems development project management, similarly defined risk management as "uncertain future conditions or circumstances that may adversely impact a project if they occur" (2003).

Academic views can be more abstract or even more specific. Cervone's general overview of project risk management (2006) offers the somewhat humorous definition of risk as "a problem that has not happened – yet." Olsson (2008) reviews several authors' opinions and provides a range of definitions; including "an exposure or a probability of occurrence of a loss", "a barrier to success", as being "related to concepts of chance such as the probability of loss or the probability of ruin" and even the more positive view that risk can be exposure to loss or gain. Specific examples include Elky (2006) who regards information technology security risk as anything detrimental to information that emanates from determined or unintended events that cause an untoward impact on the information. Risk can also be thought of as a function of the possibility or probability that a given threat-source can impose or have a potential negative impact on the project development life cycle.

Murray and Hillson (2008) demonstrate that risk attitude may also be a factor in effective risk management, as illustrated in Figure 1 below:

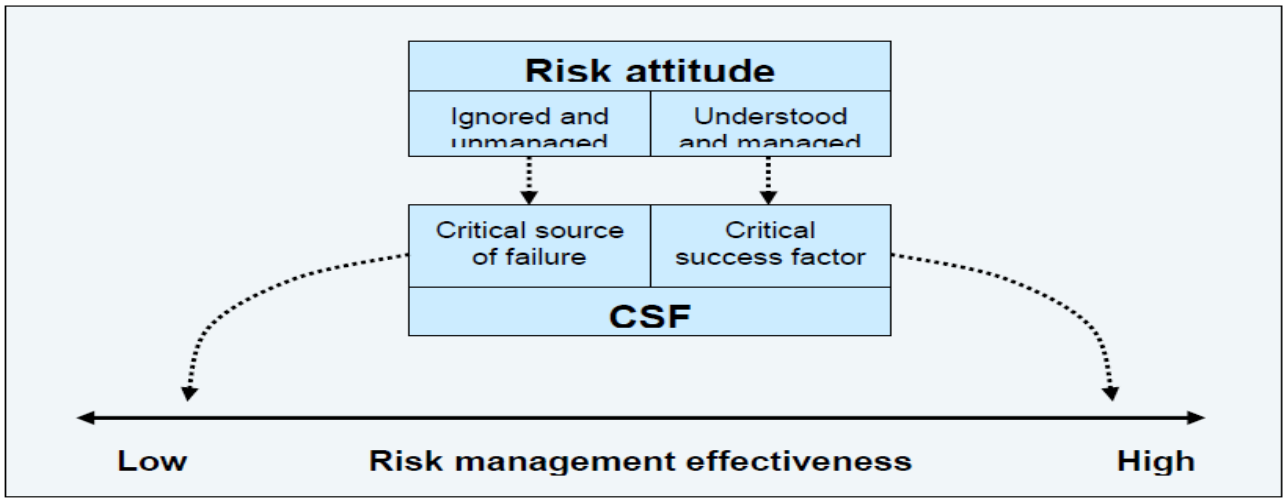

Figure 1. sk Attitude as a CSF (Murray and Hillson, 2008, p. 12

II. RISK IMPACT

Risk impact is another important dimension. According to Kajko-Mattsson and Nyfjord (2008), the risks in large IT systems development will lead to increased time deadlines, increased costs, and reduced quality of the final delivered products. Ultimately the risks will cause lost business and market share. Each risk will be associated with two parameters, risk probability and risk loss, that combine to form the risk impact (RI). This is the dependent variable in this research. RI is variable and depends on both the impact and the probability of the risk. According to the Association of Project Management (APM) and the Project Management Institute, these values can be calculated as a product of the probability of an unsatisfactory event and the loss from an unsatisfactory outcome (APM, 1997; PMI, 2000.

III. LOSS DISTRIBUTION

Loss distribution is a concept that is important to the identification, quantification and mitigation of risk. Risk management in the IT industry can vary. Large IT systems are prone to many risk factors and the quantification of the risk is very important in order to mitigate the risk in the development of secure IT systems. According to Navarrete (2002), there is a need for the IT companies to dedicate resources to manage the operations and thus implement risk management in maintaining the operational risks. The research paper produced by Navarrete (2002) explained that the losses incurred by an IT system were because of the internal weaknesses and inefficiencies and there are no standard ways of identifying them very easily. However the introduction of DRiMaP models introduced by IBM made it very easy to handle the risks in managing the IT systems. DRiMaP models are more concerned about the improvement of the quality of the systems which will in turn help to reduce the operational risks.

According to Navarrete (2002), any risk distribution will depend on the events that are defined for calculating the risk. In this section, the research is interested to explain the methodology to calculate the loss distributions in the IT systems (distributed). Any risk will be associated with the capital flow, resources available and the technology in the IT systems.

Before measuring the risk, a confidence level needs to be established so that the solution to a particular risk can be defined. It is an industry practice to set the confidence level close to 100% even though this is not practical. This is incorrect since a confidence level of 100% chosen for calculating the loss distributions will require an unacceptable and inefficient level of capital investment. A 99% confidence (certainty or point/level at which 99% of losses will be covered) will be a more acceptable as well as being helpful in understanding and calculating the loss distribution.

Expected losses (EL) and unexpected losses (UL) and operational value at risk (VAR) are helpful to understand the loss distribution patterns in the IT systems. According to Navarrete (2006), there will be always a scope for the expected losses in any IT systems whereas unexpected losses cannot be predicted earlier and contribute to the risks of the IT systems. However the unexpected losses can be calculated by the difference between the VAR and the expected losses so as to identify the future capital requirements required for mitigating the risk in the IT systems. If the unexpected losses are calculated then there will be fair chances of identifying the risks and can be distributed among the different departments in an IT system. The graph in Figure 2 depicts the expected and unexpected distribution of IT systems losses that may occur.

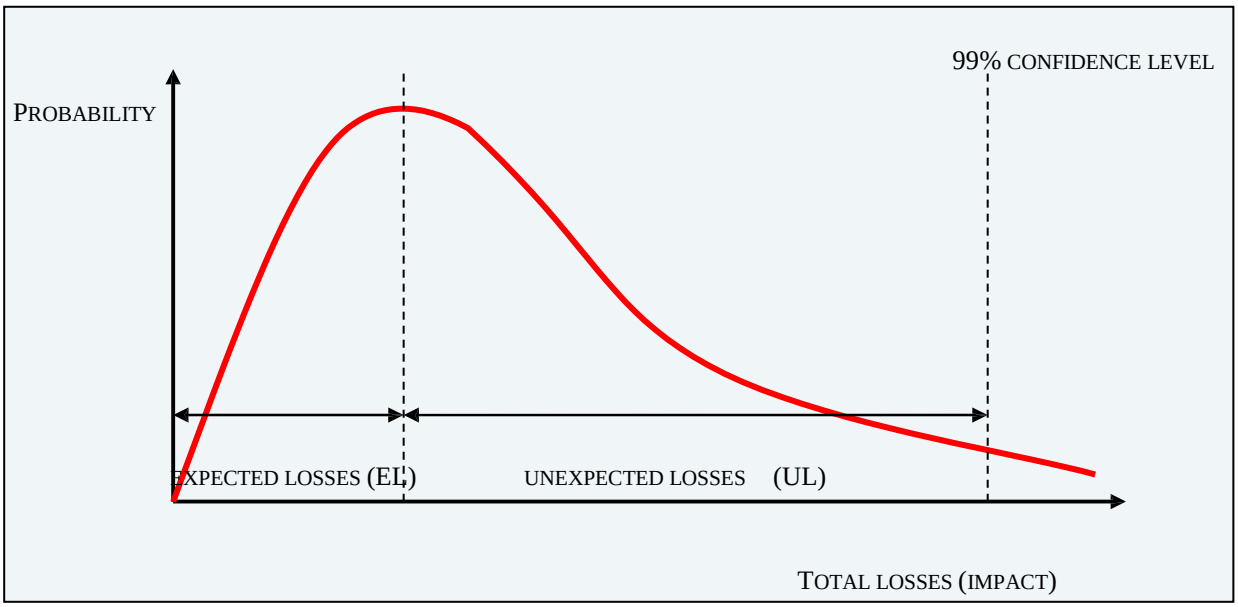

Figure 2. Project loss distribution curve for IT systems (Navarrete, 2006, p.2)

IV. RISK MANAGEMENT

Literature describes risk management in various ways. It may be treated as something philosophical, such as Kloman's (1990) definition of "a discipline for living with the possibility that future events may cause adverse effects". It can also be more specific, such as the APM (2011) definition: "Project risk management is a structured process that allows individual risk events and overall project risk to be understood and managed proactively, optimising project success by minimising threats and maximising opportunities."

Risk within organisations takes on different forms and causes. Some of them can be large in scope and potentially affect the entire organisation – a crisis. Few organisations have the infrastructure or resources to deal with crises. Mills and Walle (2007) revealed that ability to respond to such occurrence is not an indication of reduction in the damage rather a plain necessity for survival. In research conducted by the Spillan and Hough (2005) and American Management Association (AMA) according to Latto (2007) revealed that not less than 40% of organisations have no risk management plan in place. It is however shown that small firms place high emphasis on risk management plan. Mitroff et al. (1989) pointed out why most organisations do not emphasise risk management plans prior to project development and implementation. These can be a perception that a crisis is very unlikely, or reliance on insurers to cover losses. They also found that organisations that disregard the possibility of a crisis also often fail to make provision for risk management.

V. RISK MANAGEMENT AND INFORMATION TECHNOLOGY

Scope of this research covers risk in information technology projects, particularly large projects, and this section examines risk and its management in that field

A. Risk management and software processes

Software risk management (SRM) techniques may be classified as either software acquisition or software development. In large projects both types may co-exist.

Higuera and Haimes (1996) showed a basic methodological framework to manage functions may be composed of the Software Acquisition-Capability Maturity Model (SA-CMMSM) and the Software Capability Maturity Model (SW-CMMSM) and their supporting practices and constructs. This framework is supported by three groups of practices (Higuera and Haimes, 1996): Software Risk Evaluation (SRE), Continuous Risk Management (CRM) and Team Risk Management (TRM). According to this model, two additional visions or dimensions ought to be included: the temporal and human dimensions.

Achievement, growth, and exploitation programs continue to experience great cost overruns, calendar delays, and poor technical quality. These are a result of failing to deal appropriately with uncertainty in the acquisition and development of complex, software-intensive and software-dependent systems. Further studies in Higuera and Haimes (1996) revealed that potential sources of software risks involve technology, software, hardware, cost, people and schedule. These are shown in Figure 3 below:

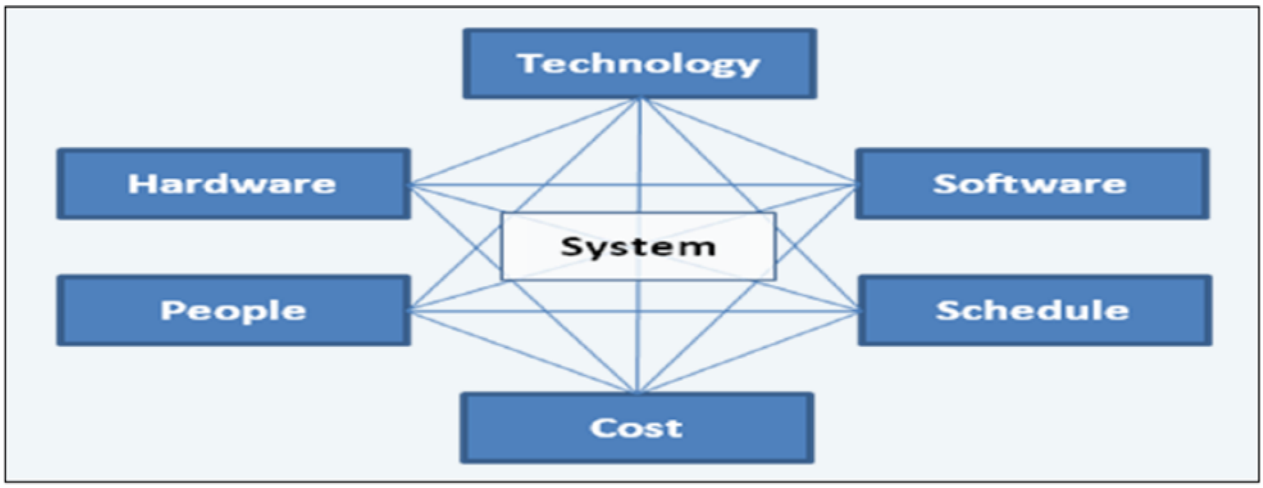

Figure 3. Risks within a system context (Higuera and Haimes, 1996)

Business needs are essential in laying a base for a discussion about the role of risk management in information systems (Gibson, 1997). Gibson gave three needs to comprehend the role of information system in risk management:

a) Most firms are measuring risk to understand the risks they are taking, such as the quantifiable examples of market risk and credit risk.

b) Risk-adjusted performance leads to better promotion of business units and individuals.

c) Risk management provides shareholders with consistent and superior risk-return exchange over time; firms match the capital they employ to the risks they take.

Gibson also revealed that firms have developed refined risk measuring techniques and make considerable investments in risk management information systems that meet their requirements. Managers expect a risk management information system to provide data they need to meet the three business needs highlighted above. Gibson showed managers expect risk management systems to:

i. Calculate value at risk.
ii. Perform scenario analyses.
iii. Measure current and future exposure to stakeholders.

Do all of the above at varying levels of aggregation; across various groups of risks, product types and stakeholder groups.

B. Strategic risk management relating to IT

Strategic risk exposes organisations to potential losses and at the same time provides them with a number of opportunities. Most IT companies invest large amounts on their operating systems and technologies, so their key objectives would include investing in technologies that will enhance their strategic advantage. In order to gain strategic advantage the organisation must eliminate critical risks and determine how to survive and succeed in business (Wallis, 2005). This can be achieved by focussing on any financial and operating flexibility that may help the technological base, operations or financial structure adapt in response to the changed environment. In so doing the organisation will be more agile in an uncertain environment and take faster advantage of opportunities.

VI. CONCLUSION

Risk management is a key component for project cost estimating and scheduling. The power of risk management will be completely realised whenever a project manager takes action to respond to the identified risks based on the risk analysis. In an IT project, understanding the project risks will enable the project teams to contribute to fulfilment by assessing the project risks and making the correct project development and delivery decisions. Managers must consider the resources needed for project risk management and build this into their project development budget and schedule (Twain, 2010).

Information technology projects are frequently planned and executed as a series of phases. This helps with the logical planning process, control of execution, testing and even business issues like interim signoff and payment. This research intends to offer suggestions that will be helpful to project managers and software developers throughout the project lifecycle. These participants will understand the major risks associated with IT and software development projects and enable them to plan, organise, direct and control the software project

REFERENCES

[1] APM (2011) APM Body of Knowledge 5th Edition, APM Definitions, online at www.apm.org.uk/sites/default/files/Bok%20Definitions.pdf

[2] Olsson, R. (2008) "Risk management in a multi-project environment: An approach to manage portfolio risks", International Journal of Quality & Reliability Management, Vol. 25 No. 1, 2008 pp. 60-71

[3] Elky, S (2006) "An Introduction to Information System Risk Management", SANS Institute, online at www.sans.org/reading_room/whitepapers/auditing/introduction-information-system- risk-management_1204

[4] Murray, R. and Hillson, D. (2008) Managing group risk attitude, Gower Publishing Ltd.

[5] Kajko-Mattsson K. and Nyfjord J., (2008) "State of Software Risk Management Practice", IAENG International Journal of Computer Science, Vol. 35, No. 20

[6] APM (1997) "Association for Project Management Project Risk Analysis and Management Guide (PRAM Guide)", APM Risk Specific Interest Group

[7] PMI (2000) Project Management Institute Guide to the Project Management Body of Knowledge (PMBOK)

[8] Kloman, H.F. (1990) "Risk management Agonistes", Risk Analysis, Vol. 10, No. 2

[9] Mills, K. and Walle, B. (2007) "IT for Corporate Crisis Management: Findings from a Survey in different Industries on Management Attention, Intention and Actual Use", Proceedings of the 40th Hawaii International Conference on System Sciences – 2007, pp 24, January, Hawaii

[10] Spillan, J.E. and Hough, G.M. (2005) "Crisis Planning: Increasing Effectiveness, Decreasing Discomfort", Journal of Business and Economics Research, Vol. 3, No. 4, pp. 19-24 Standish Group (1994) CHAOS Report, The Standish Group, USA

[11] Latto, A. (2007) Managing risk from within: monitoring employees the right way, Cengage Learning, Gale, USA

[12] Mitroff, I., Pauchant, T., Finney, M. and Pearson, C. (1989) "Do some organisations cause their own crises? The Cultural profiles of crisis-prone vs. Crisis-prepared organisations", Industrial Crisis Quarterly 3, pp. 269 – 283

[13] Higuera, R.P. and Haimes, Y.Y. (1996) Software Risk Management: Technical Report, Carnegie Mellon University, Pennsylvania

[14] Gibson, M. (1997), "Information systems for risk management: Federal Reserve Board", online at www.bis.org/publ/ecsc07f.pdf

[15] Wallis, M.R., (2005), "Corporate risk taking and performance", online at pages.stern.nyu.edu/~adamodar/pdfiles/papers/strategicrisk.pdf

[16] Twain, M. (2010) Project Risk Management, online at www.wsdot.wa.gov/publications/fulltext/cevp/ProjectRiskManagement.pdf