Task Oriented Risk Assessment (TORA)

M.Lahon*
Department of CS and IT
Don Bosco College of Engineering and Technology
A Constituent Unit of Assam Don Bosco University
*Working with Department of CSE, AEI

Y.Jayanta Singh
Department of CS and IT
Don Bosco College of Engineering and Technology
A Constituent Unit of Assam Don Bosco University

ABSTRACT

This study explores the need for risk assessment and also gives an overview of some standard risk management frameworks. A new task oriented framework is introduced which will help to identify the risk associated in fulfilling any objective or solving any possible problem. The approach proposes to make a common guideline to identify and assess the risk associated in any kind of organisation or project, and assists in identifying those events which require more attention in case of managing risk.

General Terms

Uncertainty, Risk management, risk analysis, risk assessment.

Keywords

Project, Task, Event, Risk framework, Impact, Risk Exposure

1: INTRODUCTION

Every organisation uses the concept of the term “Project”. To progress every organisation has to take up projects of smaller or bigger magnitude. For successful completion of a project, formal project management principles and techniques are designed. The basic steps for effective project management includes: scheduling, estimation of cost, risk management and project closure analysis.

Risk management consists of risk identification, analysis and assessment, risk projection, monitoring, mitigation and management [2]. It plays a critical role as it is associated with uncertainty. Risk is associated with two characteristics – uncertainty and impact. Uncertainty is ascertained using the concepts of probability of occurrence of a particular event whose measure is greater than 0 and less than 1. Impact relates to the severity of the event which may be categorized or scaled into a set of three, four, five or more classes where each class may be termed as critical, marginal, catastrophic etc. depending on the situation.

There are various categories of risk which includes project risk, technical risk, and market risk as a known or unknown risk. Historical studies provide certain assistance in assessing risk [4]. Due to the changing external factors risk analysis is required as a form of an integral part of every project management plan as well as any organisation. This analysis will take up the risk mitigation measures that can reduce the probability of cost and time overrun which in turn will minimise wastage of valuable resources.

2. STUDY ON FRAMEWORKS

There are various frameworks available which can form the basis of risk management. Our study has included the following important frameworks which are considered as the basis for the new framework that is explained later.

2.1. COSO

This framework emphasises on risk management of the entire enterprise to achieve an entity’s objectives, set forth in four categories as - Strategic, Operations Reporting and Compliance. These objectives are to be achieved with the help of the eight different components of Enterprise Risk Management-Internal environment, Objective setting, Event identification, Risk Assessment, Risk Response, Control Activities, Information and Communication and Monitoring [7]. It represents the relationship between the objectives, components and the entity units. It gives the ability to focus on the entirety of an entity’s enterprise risk management or by objective category, component, entity unit, or any subset thereof.

2.2..Australian/New Zealand Standard AS/NZS 4360:1999 and AS/NZS 4360:2004.

The Australian-New Zealand framework introduced the concept of “Context” which provides the essential linkage between decision-makers and the technical or scientific analysis of risks. It can be described as a process to “Establish the strategic, organizational and risk management context in which the rest of the process will take place. Criteria against which risk will be evaluated should be established and the structure of the analysis defined” [1].

AS/NZS 4360:2004 revised standards incorporate following:
(a) Places greater emphasis on embedding risk management practices in the organization’s culture and processes;
(b) Considers the management of potential gains as well as potential losses.

2.3. Structured Approach based on COSO and ISO 31000 frameworks*:*

In order to successfully implement, support and sustain the risk management process, a structure is required. ISO 31000 considers the risk management process as a list of co-ordinated activities. Some of the important processes are:- identification of risks, evaluation of risks, responding to significant risks, tolerate, treat, transfer, terminate, resource controls, reaction planning, and reporting and monitoring risk performance and reviewing the risk management Framework etc. ISO 31000 describes a framework for implementing risk management, rather than a framework for supporting the risk management process [6].

2.4. National Institute of Standards and Technology Special Publication (NIST) 800-30

According to this guide risk management process for IT systems is implemented to minimise the negative impact and fulfil the need for a basis in decision making. The risk management methodology is the same regardless of the Software development life cycle (SDLC) phases for which the assessment is being conducted. Risk management is an iterative process that can be performed during each major phase of SDLC. Identifying risk for an IT system requires a keen understanding of the system's processing environment. To conduct risk assessment, first system-related information is to be collected, which is usually classified as follows- Hardware, Software, System interfaces (e.g., internal and external connectivity), Data and information, Persons who support and use the IT system, System mission (e.g., the processes performed by the IT system), System and data criticality (e.g., the system's value or importance to an organization), System and data sensitivity [11].

2.5. NERAM (Network for Environmental Risk Assessment and Management) Framework, 2003

According to this the basic functions involved in risk assessment and treatment and the linkages to the high level risk management framework comprises of three processes given below[1]. The three main processes are:
(a) Risk Estimation to estimate the magnitude of the risk (probability and consequences).
(b) Evaluation to compare the estimated risk against criteria such as costs, benefits, stakeholders concerns.
(c) Treatment Options that are developed to reduce the risk to an acceptable level.

3. SUMMARY OF THE STUDIED FRAMEWORKS

All the concepts discussed in the above frameworks can be summarised and a set of activities for risk identification, assessment and control can be given as follows:

(a) Identify the need of the stake holders.
(b) Identify the threats or vulnerabilities/risk.
(c) Assess/Evaluate the risk.
(d) Establish control points to minimise risk.
(e) Implement risk control measures.

4. TASK ORIENTED RISK ASSESSMENT (TORA)

This new framework is proposed for risk identification and assessment and can form a basis for the decision makers to initiate risk control measures. This in turn can assist in identifying the critical points where the management needs to emphasise to avoid disaster or loss. Risk management starts with risk identification then risk assessment and finally risk control and mitigation measures. In our study we have concentrated on risk identification and risk assessment. The exercise of risk identification and assessment is a proactive exercise rather than reactive and so always has a component of uncertainty. Assessment can be either qualitative or quantitative [3], [8]. The proposed framework can identify the risks based on the tasks identified to fulfil the objective or solve the problem.

This study concentrated more on the identification of the risk using a standard concept of task identification. Every objective to be fulfilled can be broken down into tasks. These tasks are further broken down into subtasks. The risk can also relate to each of these subtasks. According to the framework each subtask is identified and the possible event which may cause the subtask to fail is also identified. Each of these events will have a probability of occurrence which can be determined from historical information or from estimated risk related data. In cases where exact probability cannot be determined qualitative measures can be provided.

To determine the risk exposure in case of some failing subtask, the impact of the failure needs to be determined. The impact of the failure can be categorised as negligible, marginal, critical or catastrophic. Impact of failure can also be expressed in terms of loss in cases where loss can be quantified. The proposed TORA framework for risk identification and assessment can be represented with the following diagram where each of the oval and squares represents activities which are given in details below:

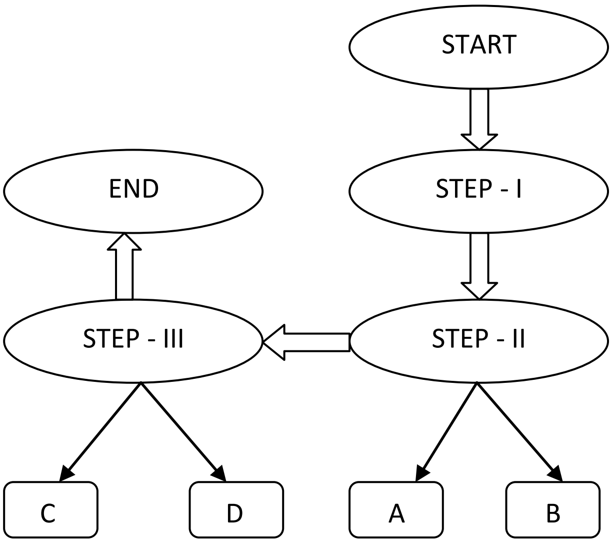


Figure 1: Task Oriented Risk Assessment (TORA) Framework

The Framework starts with the goals and objectives to be fulfilled and forms the starting point of risk identification and ends with the risk assessment of the identified risks which can form a ready reference for the decision makers to introduce the monitoring and control measures and thus make a directed effort to minimise losses.

Detailed descriptions of the steps in TORA

START: Goals/objectives of the organisation/project/ scheme/department/section

(a) STEP I: Preparation of the tasks and subtasks to accomplish the goals/objectives.
(b) STEP II: Identify the risks associated with each subtask.
A: Find the events that can cause failure of the subtask.
B: Find the probability of occurrence of each of the event.

(c) STEP III: Analyse the consequences against each identified risk in terms of the entity to be affected and find a measure of the impact.

C: Find the entity to be affected when the event occurs.

D: Identify the severity of the impact caused by the event.

(d) END: Interpret and present the results of the analysis in the form of reports /graphical aids.

Advantage of TORA framework is that it is based on task and subtask analysis and it does not need any risk analysis expert to identify the risk. The framework can be used in identification and assessment of risk in any organisation without giving any extra effort and time. The risk identification activity can be merged with the task identification activity.

Each task will comprise of one or more subtasks. Each of the subtasks can then be processed to calculate the risk exposure. This can be estimated by making a list of the events which could cause the subtask to fail. Each of the events will have a probability of occurrence and an amount of impact. Impact can be either given in terms of qualitative or quantitative measure. In case of qualitative measure the impact on the entity can be categorised as negligible, marginal, critical or catastrophic. In case the impact on the entity can be quantified in terms of cost, effort or loss, the assessment can be termed as a quantitative risk assessment.

Once the probability and impact is ascertained for each event that can cause the sub task to fail, risk exposure of a subtask can be calculated as given in equation (1). Risk Exposure is calculated as probability of occurrence multiplied by measure of impact in this case. According to Pressman in his book on Software Engineering, Risk Exposure is expressed as (P * C) where P is the probability of occurrence and C represents the loss in terms of cost [2]. In this risk exposure calculation, the impact i.e. loss cannot be ascertained in terms of cost and a qualitative assessment is only possible.

$$RE_{ST} = \sum_{i=1}^{e} (P_i * I_i) \qquad \text{---} \quad (1)$$

Where,

$RE_{ST:}$ Risk Exposure for each subtask (ST),

P: Probability of occurrence of each event i,

I: Impact on entity for each event i

e: Total nos. of events that may lead to the failure of ST.

Total risk exposure of a task can be calculated as

$$RE_T = \sum_{ST=1}^{T} RE_{ST} \qquad \text{---} \quad (2)$$

Where RE_T is the Risk Exposure for task T.

In cases where probability cannot be determined as a crisp value, fuzzy logic concept can be used for assessing the risk. It is possible to get the response to frequency of occurrence can be categorised as frequent, likely, most likely etc. and impact may be described as catastrophic, critical, marginal etc. To incorporate these responses fuzzy logic is a suitable alternative for risk assessment [9, 10].

5. EXECUTION OF TORA

To execute the concept of TORA we have take the real live processes of one LPG bottling plant in Assam, India. The objective of the bottling plant is to fill in the LPG cylinders with accurate weight having no leakage. Among the objectives of bottling plant that has many tasks and sub tasks, our study has taken two tasks for execution using TORA.

Task1: Check weight of the cylinders

This task is performed to verify that the cylinder has been filled correctly within permissible limits.

Task2: Test for tightness

This task is performed with the intention to check the leak

which may be 'SC' type valve leak or a general leak. Such

the identification tasks completes in STEP I.

Considering the first task of checking the weight of cylinders, there are two possibilities which may cause the task to fail. If the weight is within the acceptable range then the task is a success or else the task fails. The weight could be overweight or underweight. The conditions are termed as

(a) overfilled or
(b) under filled

When we go for risk assessment the probability of each of the event is to be ascertained. We have considered that the exact probability could not be ascertained and a qualitative assessment is obtained from the expert in each of the case [4], [5]. An assessment criterion is considered by introducing the frequency of occurrence of failure in terms of most likely, likely and unlikely. This is only a measure for execution and may include other intermediate steps for more accurate assessment of frequency. For the given example we have considered the following:

(a) Overfilled: unlikely
(b) Under filled: most likely

The frequency of occurrence is to be given some numerical value so as to enable the calculation of Risk Exposure and for the purpose of representation using graphical aids. We have considered - 'unlikely' to be 1, likely to be 2 and most likely to be 3. This concludes the activities in STEPII of the framework.

The activity in STEP III of the framework intends to identify and quantify the impact of the failures identified in the previous step. For qualitative assessment the impact is assessed in five categories: catastrophic, critical, marginal, and negligible and no impact. This can be quantified by assigning 5 for catastrophic, 4 for critical and so on.

There is another point which needs to be specified i.e. when do we ascertain the impact to be catastrophic or critical or no impact. This can be defined by the organisation as this framework is intended for any type of organisation and nothing can be made rigid in this case. This also depends on the risk acceptance capacity of the organisation, project, scheme etc.

During the execution of TORA under such condition we have considered the harm(s) that may lead to human death or permanent disability and major environmental disaster as catastrophic, major injury and non repairable damage to equipments and factory to be critical, minor injury and repairable damage to factory, equipment and organisation as marginal, no impact on human and environment but minor damage to equipment and property as negligible and no impact on human, environment or property as no impact. In this case if the cylinder is overfilled, impact is catastrophic and if under filled impact is marginal and is represented in tabular form as follows:

Events for task1	**Frequency of occurrence**	**Impact**
1. Cylinder overfilled	unlikely	catastrophic
2. Cylinder under filled	most likely	marginal

The risk exposure RE of event1 and 2 can be represent as

$RE_1 = 1 * 5 = 5$

$RE_2 = 3 * 3 = 9$

Therefore the total RE for the task1 (event 1 and 2) is:

$RE_{task1} = 5 + 9 = 14$

Now we consider the second task i.e. checking for tightness. There are two events that may cause the failure of this task i.e. a valve leak or a bung leak. Failure of this task means that there is a leak detected.

Considering the same criteria as in the previous task, the RE for task 2 is identified as follows:

Events for task 2	**Frequency of occurrence**	**Impact**
1. Valve leak	most likely	critical
2. Bung leak	unlikely	catastrophic

In terms of figures we can express as follows:

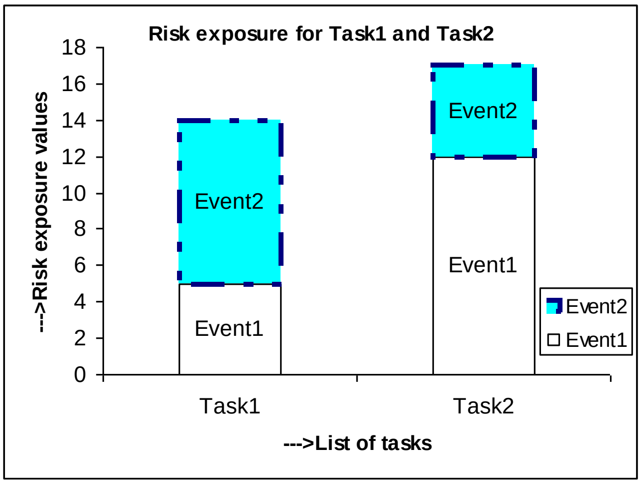
$RE_1 = 3 * 4 = 12$

$RE_2 = 1 * 5 = 5$

There RE for the task no. 2 is:

$RE_{task2} = 12 + 5 = 17$

In both the cases we have considered two events that may cause failure of the task. A limit of 2 events is considered for execution, which may be increased depending on the modes of failure of the tasks of the organisation. This is necessary to make a common base for graphical representation. The outcomes of the study can be represented as below:



This representation indicates the risk exposure of the two tasks which can form a ready reference to identify those tasks which needs more analysis to initiate or intensify the risk control measures. The events which cover larger areas need more attention. Therefore it is understood that Risk Assessment must form an integral part of every organisation, project, scheme etc. so as to identify those tasks and events which require further risk monitoring and control measures to minimise loss of any form.

6. CONCLUSION

The study of the different frameworks reveals that risk management starts with the identification of risk, then analysis and assessment and finally risk monitoring and control measures.

The proposed TORA framework considers only risk identification
and assessment. Risk identification is performed considering the different tasks and the events that may cause its failure with its impact. The framework is simple to implement and will help to identify the events that are more vulnerable and needs more attention. This in turn will minimise the impact that could have happened if this analysis was not done to identify the critical points which are exposed to risk. Risk analysis and assessment should form an integral part of every organisation so as to minimise the loss in terms of resources which could be human, natural or financial.

7. REFERENCES

[1] J. Shortreed, J. Hicks, L. Craig, ‘ Basic Frameworks for Risk Assessment’ Report prepared for the Ontario Ministry of Environment, March’2003.

[2] R.S. Pressman, Software Engineering, 5th Edition, McGRAW-HILL

[3] ‘A Guide By The Association For Project Management’ , Compiled from information provided by members of the Special Interest Group on Risk Management, Jan 2000.

[4] N. E. Fenton and M Neil, ‘The use of Bayes and causal modelling in decision making, uncertainty and risk ‘, 2 June 2011.

[5] T. Aven, ‘Risk Analysis: Assessing Uncertainties Beyond Expected Values and Probabilities’ , John Wiley & Sons, Ltd, 2008.

[6] A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000, © AIRMIC, Alarm, IRM: 2010

[7] COSO (Committee of Sponsoring Organisations of the Treadway Commission), ‘Enter-prise Risk Management: Integrated Framework’, www.coso.org/publications.htm, 2004

[8] ”Enterprise Risk Management: Tools and Techniques For Effective Implementation”, Published by IMA, 2007.

[9] Z. Plamena, P.Lyubka, S. Krasimir, V.Dimiter, “Fuzzy Logic Model for Natural Risk Assessment in SW Bulgaria”, 2nd International Conference on Education and Management Technology, IPEDR vol.13 (2011) IACS IT Press, Singapore

[10] B .Pradhan and S. Lee , ‘Landslide risk analysis using artificial neural network model focussing on different training sites’, November 2008.

[11] G Stoneburner , A Goguen and A Feringa , “Risk Management Guide for Information Technology Systems”, Recommendations of NIST, 2002