Software Risk Management

Engr. Shehnila Zardari
Lecturer, Department of Computer Science & IT.
NED University of Engineering and Technology,
Karachi, Pakistan
e-mail: shehnilaz@gmail.com

***Abstract*— Building and maintaining software is a risky business. Since software permeates and controls so much of the present-day enterprise (and its products), delay, cost excess, and failure to fulfill a command, can have far-reaching consequences. A common response to such risk is to ignore it completely. We justify this as "positive approach," the heart and soul of a Can-Do management philosophy. But when real risks turn into real problems and throw our projects down in flames, we can see that our past "positive approach" was little more than repudiation. There should be a better way.**

Planning the core activities, the must-be-dones of software development, is an essential but not sufficient beginning. Given that projects never run just exactly as the optimal plan, we need Risk Management as well. Risk Management is project management for adults. It keeps your attention focused constructively on the very characteristics that, if overlooked, could lead to disastrous collapse of the project.

A policy of risk aversion guides us to become more and more efficient and to avoid things that are less and less worth doing. The projects that yield real benefit are destined to be full of risk. Running away from risk will not prove to be useful instead we need to school ourselves to run toward it, but very, very cautiously.

As high benefit endeavors are always risky, we have to make ways to find out the lurking risks, estimate their effect, optimize our response, and keep an eye on the changes. These are the vital skills of Risk Management.

Keywords; Software Risk Management

I. RISK

Risk is defined as “Hazard, danger; exposure to mischance or peril.” [1]. A simple definition of Risk is: “The possibility of loss, injury, disadvantage or destruction.” [6]

II. RISK MANAGEMENT

Risk Management consists of the processes, methodologies and tools that are used to deal with risks in the Software Development Life Cycle (SDLC) process of a Software Project. Risk Management is defined as the activity that identifies a risk; assesses the risk and defines the policies or strategies to alleviate or lessen the risk. "Risk management is simply a practice of systematically deciding cost effective approaches for minimizing the outcome of threat realization to the organization. It can also be defined as "a project management tool to assess & tone down the events that might adversely affect a project, thereby increasing the possibility of success."

III. RISKS IN SOFTWARE PROJECT MANAGEMENT

Unlike the hazards of daily living, the dangers in the young and rising field of software engineering must often be learned without the help of lifelong exposure. A more intentional approach is required. Such an approach includes studying the experiences of successful project managers and keeping up with the leading writers and thinkers in the field. The top software risk items can be [8]:

1) Personnel Shortfalls
2) Unrealistic schedules and budgets
3) Developing the wrong functions and properties
4) Developing the wrong user interface
5) Gold-plating
6) Continuing stream of requirements changes
7) Shortfalls in externally furnished components
8) Shortfalls in externally performed tasks
9) Real-time performance shortfalls
10) Straining computer-science capabilities

IV. PROACTIVE AND REACTIVE RISK MANAGEMENT

Risk management focuses to assess the probability of risk occurring, risk event drivers, risk events, the probability of impact and the impact drivers before the risk actually takes place. This is in fact called ‘proactive risk management’. Fig. 1 shows the flow of Proactive Risk Management.

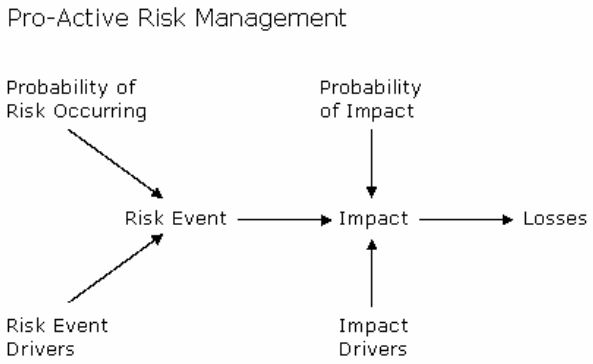

Figure 1. Proactive Risk Management

978-0-7695-3595-1/09 $25.00 © 2009 IEEE
DOI 10.1109/ICIME.2009.138

When a Project team responds to risks when they occur then it is called 'reactive risk management'. Failures are fixed; resources are found and applied once the risk strikes.

V. RISK MANAGER

The role for this position is to highlight and capture the risk and formalize risk management activities and results. This role includes being spokesperson for the program for risks for important reviews and reports. It is the responsibility of Risk Manager to make the Risk Management plans, evaluate and verify risks and even monitor the status of the risks process of Software Projects. A Risk Manager should be able to anticipate the risks, evaluate the risks and define measures to mitigate them ably.

VI. RISK MANAGEMENT PROCESS OVERVIEW

The following diagram illustrates the six steps of the risk management process: identify, analyze and prioritize, plan and schedule, track and report, control, and learn. It is imperative to know that the process of managing each risk goes through all of these steps at least once, and often cycles through numerous times. Also, each risk has its own timeline, so there might be multiple risks in each step at any point in time. Fig. 2 shows different steps involved in managing risk. Below is a brief introduction to the six steps of the risk management process:

A. Identify:

The purpose behind identifying the risk is to consider risks before they become problems and to incorporate this information into the project management process. Anyone who is working in a project can identify risks to the project. Each individual has some particular knowledge regarding different parts of a project. During Identify, uncertainties and issues relevant to the project are transformed into distinct (tangible) risks that can be described and measured.

During this function, all risks are written with the two part format. The first part is the risk statement, written as a single statement concisely mentioning the cause of the concern and its impact.

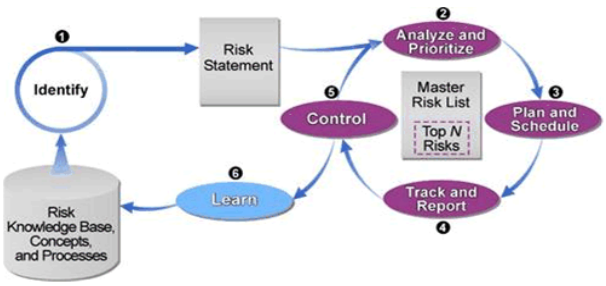

Figure 2. The process of managing risk

The second part may include additional supporting details in the form of a context.

The aim for a risk statement is that it be clear, concise, and contains sufficient information so that the risk is easily understood. Risk statements in standard format must contain two parts: the condition and the consequence. The condition-consequence format provides a complete picture of the risk, which is critical during mitigation planning. [9] It is read as follows:

given the <condition> there is a possibility that <consequence> will occur

A diagram of the complete risk statement and context are shown in Fig. 3

B. Analyze and prioritize:

The purpose of Analyze is to transform the data into decision-making information. Analysis is a process of examining the risks in depth to determine the magnitude of the risks, how they relate to each other, and which ones are the most important. Analyzing risks has three basic activities: evaluating the characteristics or attributes of the risks (impact, probability, and timeframe), classifying the risks, and prioritizing or ranking the risks.

Evaluating - The first step gives better understanding of the risk by qualifying the expected impact, probability, and timeframe of a risk. This includes establishing values for:

- Impact: the loss or negative effect on the project if the risk occur
- Probability: possibility that the risk will occur
- Timeframe: the period when you must take action so as to mitigate the risk

Table 1 describes sample values that might be used to evaluate a risk's attributes

Prioritizing the risk is the last step in the Analysis function. The objective is to sort through a large number of risks and determine which are most important and to separate the risks which should be dealt with first (the vital few risks) while allocating resources. This involves partitioning risks or groups of risks based on the "vital few" sense and ranking risks or sets of risks based on continuously applying an established set of criteria. No project has unlimited resources with which it can mitigate risks.

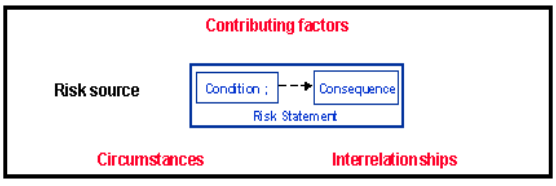

Figure 3. Risk Statement & Context

Therefore, it is essential to determine consistently and efficiently which risks are most important and then to focus those limited resources on mitigating risks.

TABLE 1. SAMPLE ATTRIBUTE VALUES

Attribute	Value	Description
Probability	Very Likely (H)	High chance of this risk occurring, thus becoming a problem > 70%
	Probable (M)	Risk like this may turn into a problem once in a while {30% < x < 70%}
	Improbable (L)	Not much chance this will become a problem {0% < x < 30%}
Impact	Catastrophic (H)	Loss of system; unrecoverable failure of system operations; major damage to system; schedule slip causing launch date to be missed; cost overrun greater than 50% of budget
	Critical (M)	Minor system damage to system with recoverable operational capacity; cost overrun exceeding 10% (but less than 50% of planned cost
	Marginal (L)	Minor system damage to project; recoverable loss of operational capacity; internal schedule slip that does not impact launch date cost overrun less than 10% of planned cost
Timeframe	Near-term (N)	Within 30 days
	]	
	Mid-term (M)	1 to 4 months from now
	Far-term (F)	more than 4 months from now *NOTE: refers to* ***when action must be taken***

Conditions and priorities keep on changing during a project, and this natural evolution can affect the important risks to a project–. ***Risk analysis must be a continual process***. Open communication is required for analysis so that prioritization and evaluation is accomplished using all known information. A forward-looking view allows personnel to consider long-range impacts of risks.

C. Plan and schedule:

"Planning is the function of deciding what, if anything should be done about a risk or set of related risks." [10] In this function decisions and mitigation methods are developed based on current knowledge of project risks.

The purpose of plan is to:

- make sure the affects of the risks and their sources are known
- develop effective plans
- plan efficiently (only as much as needed or will be of any benefit)
- produce, over time, the correct set of actions that minimize the impacts of risks (cost and schedule) while maximizing opportunity and value
- plan important risks first

Fig. 4 indicates the potential approaches to Risk Planning.

There are four options to consider while planning for risks:

1) *Research:* make a plan to research the risk.
2) *Accept:* decide to "accept" the risk and document the cause behind the decision
3) *Watch:* monitor risk conditions for any signs of change in probability or impact.
4) *Mitigate:* allocate resources and assign actions so as to minimize the probability or potential impact of risks. This can range from simple tasking to difficult and major activities:

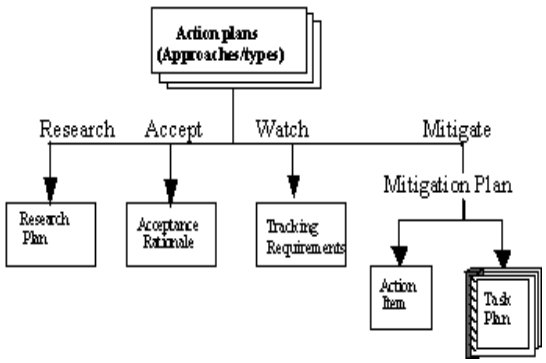

Figure 4. Planning approaches

- Action Items are a series of individual tasks to mitigate risk
- Task Plan formal, well-documented and larger in scope.

Dealing with risk is a continuous process of determining what to do with new concerns as they are identified and efficiently putting the project resources into use. An integrated approach to management is required to make sure that the mitigation actions do not conflict with project or team plans and goals. A shared product vision and global perspective are needed to create mitigation actions on the macro level to the benefit the project, customer and organization. The focus of risk planning is to be forward looking, to prevent risks from becoming problems. Teamwork and open communication enhance the planning process by increasing the amount of knowledge and expertise that can be applied to the development of mitigating actions.

D. Track and report

Risk tracking monitors the status of specific risks and the progress in their respective action plans. Risk tracking also includes monitoring the probability, impact, exposure, and other measures of risk for changes that could alter priority or risk plans and ultimately the availability of the service. Risk reporting ensures that the operations staff, service manager, and other stakeholders are aware of the status of top risks and the plans to manage them.

E. Control:

Risk control is the process of executing risk action plans and their associated status reporting. Risk control also includes initiating change control requests when changes in risk status or risk plans could impact the availability of the service.

F. Learn:

Risk learning formalizes the lessons learned and uses tools to capture, categorize, and index that knowledge in a reusable form that can be shared with others. Learning in other words mean to ***communicate and document*** the risks for *all* personnel to understand the project's risks and mitigation alternatives as well as risk data and to make effective choices within the constraints of the project.

VII. RISK QUANTIFICATION:

Risk needs to be quantified in two dimensions. The impact of the risk needs to be assessed. The probability of the risk occurring is needed to be assessed. For simplicity, rate each on a 1 to 4 scale. The larger the number, the larger the impact or probability. By using a matrix as shown in Fig. 5, a priority can be established. [7]

Note that if probability is high, and impact is low, it is a Medium risk. On the other hand if impact is high, and probability low, it is High priority. A remote chance of a catastrophe warrants more attention than a high chance of a hiccup. There are four things you can do about a risk. The strategies are:

- Avoid the risk. Do something to remove it. Use another supplier for example.
- Transfer the risk. Make someone else responsible. Perhaps a Vendor can be made responsible for a particularly risky part of the project.
- Mitigate the risk. Take actions to lessen the impact or chance of the risk occurring. If the risk relates to availability of resources, draw up an agreement and get sign-off for the resource to be available.
- Accept the risk. The risk might be so small the effort to do anything is not worth while.

A risk response plan should include the strategy and action items to address the strategy. The actions should include what needs to be done, who is doing it, and when it should be completed.

VIII. RISK MANAGEMENT VALUE:

Efficient risk management can constitute value in the following dimensions:

1) Compliance and prevention
   - Avoid crises in own organization
   - Avoid crises in other organization
   - Avoid personal liability failure
2) Operating performance
   - Understand full range of risk facing the organization
   - Evaluate business strategy risks
   - Achieve best practices
3) Corporate reputation
   - Protection of corporate reputation

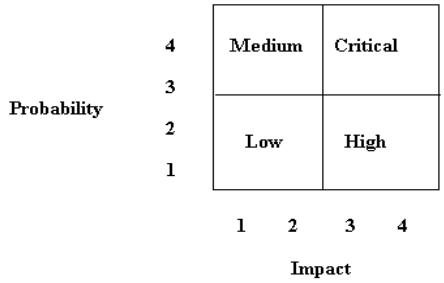

Figure 5. Risk Quantification [7]

4) Shareholder value enhancement
   - Enhance capital allocation
   - Improve returns through value based management

IX. CONCLUSION:

Thus one can conclude that formal risk management analysis and formal project assessments are effective and useful approaches that are starting to add rigor to the phrase "software engineering". Not every risk factor is fully controllable, and several risk factors exceed the authority of software managers. Nonetheless, risk analysis and assessment methods are quite effective in the identification of significant problems. Once problems are identified and examined, solutions can often be developed. We can say in conclusion that, like any other control, proper and timely Risk Management control can provide enormous advantages to an organization by cutting down on costs and ensuring proper delivery as per schedule.

REFERENCES

[1] Risk, Oxford English Dictionary

[2] Risk Management for Software: Learning to Contain, Mitigate, and Manage the Uncertainties of Software Development by Tim Lister.
http://www.cutter.com/workshops/19.html

[3] Risk Management, Introduction to Software Risk Management By Joydip Kanjilal.
http://aspalliance.com/1275_Introduction_to_Software_Risk_Management.3

[4] Reactive Risk Management
http://www.cc.gatech.edu/classes/AY2001/cs3300_fall/Slides/ch5col/sld020.htm

[5] Proactive Risk Management
http://www.valuebasedmanagement.net/methods_raroc.html

[6] Risk Manager, Risk Management by Chester Simmons.
http://home2.btconnect.com/managingstandard/risk_1.htm

[7] Risk Management Basics By Neville Turbit
http://www.baz.com/kjordan/swse625/intro.html

[8] Risks in Software Project Management.
http://www.baz.com/kjordan/swse625/intro.html

[9] Continuous Risk Management at NASA By Dr. Linda H. Rosenberg, Theodore Hammer, Albert Gallo
http://satc.gsfc.nasa.gov/support/ASM_FEB99/crm_at_nasa.html

[10] Risk Management in a Software Development Life Cycle by Anton D. Buttigieg
http://www.cis.um.edu.mt/~abut/#Section%205