

A Narrative Study on Design and Development of Risk Management Tools for Software Development

K.Adalarasan¹ Dr.R.Balu²

¹Research Scholar (Ph. D) ²Assistant Professor

^{1,2}Department of Computer Science

¹Bharathidasan University, Tiruchirappalli, Tamil Nadu, India ²Sudharasan College of Arts and Science Pudukkottai Tiruchirappalli, Tamil Nadu, India

Abstract— Risks are potential problems that may affect successful completion of a software project. Risk management is basically an approach in which we explore to identify, analyze, plan and mitigate/avoid the risks that can affect software project success. Risk management is an important part of project management which leads to the success of a project if handled efficiently. The automated risk management tools are essential to ensure the risks are managed in a globally agreed manner. It is important to select the appropriate tools for risk management based on project nature. The software development of significant software application codes is an often difficult, complicated, and sometimes uncertain process, success depends on identifying and managing risk. One of the software evolutions of software engineering, as a discipline, has been the desire to identify reliable, quantifiable ways to manage software development risks. This documentation provides a basic concepts, terminology, tools and techniques of Software Risk management.

Key words: Risk Management, Paradigm, Risk Management Tools, SDLC Software Development Life Cycle

I. INTRODUCTION

Risk is an uncertainty that can positively or negatively impact a project. Software development is a risky process; which is vulnerable to risks from the start of the project till the implementation. Each phase of the SDLC is susceptible to different sets of threat factors that might hinder the development process from being completed successfully. In order to manage these risks properly, adequate understanding on the risk management process and automated tools for risk management is required. Thus the risk factors are the uncertain conditions, which will affect the cost, duration, and quality of the project negatively. If these factors are ignored or not managed well, then it will result to a project failure. If we are dealing with uncontrollable risk then we need to set an action plan that can minimize the effect of these risks as it cannot be fully avoided. The literatures indicates that the systems without proper risk management more than 20% of all software development projects are cancelled outright before completion and something like 80% swamped their budgets. Considering all these factors in a software project, the risk management and automated tools to manage the risk is essential for project success.

II. RISK MANAGEMENT IN SOFTWARE DEVELOPMENT

The process of identifying, analyzing, planning and then mitigating or controlling the risk is known as Risk Management. Nowadays, software becoming a major part of any business. Software development is an activity connected

with advanced technologies for the implementations of business requirements. Risks on software development projects must be successfully mitigated to produce successful software systems. Lack of a defined approach for risk management is one of the common causes for project failures. . The purpose of Risk Management is to identify, assess and control project risks. Identified risks are analyzed to determine their potential impact and likelihood of occurrence. Risk management is an essential part of project management. The efficiently risk managed projects increases the chances of success up to a great extent.

III. SOFTWARE RISK MANAGEMENT PROCESS

Risk management focuses on identifying and assessing the risks to the project and managing those risks to minimize the impact on the project. There are no risk-free projects because there are infinite numbers of events that can have a negative effect on the project. Risk management is not about eliminating risk but about identifying, assessing, and managing risk. Risk management means risk containment and mitigation. First, we have to identify and plan. Then be ready to act when a risk arises, drawing upon the experience and knowledge of the entire team to minimize the impact to the project.

Risk Management comprises of following processes:

- 1) Identify the Risk: Recognize and describe risks that might affect successful implementation of the systems.
- 2) Analyze the risk: Once risks are identified, determine the likelihood and consequence of each risk.
- 3) Evaluate or Rank the Risk: Evaluate or rank the risk by determining the risk magnitude, which is the combination of likelihood and consequence. We need to make decisions about whether the risk is acceptable or whether it is serious enough to warrant immediate action.
- 4) Treat the Risk: This is also referred to as Risk Response Planning. During this step assess highest ranked risks and set out a plan to treat or modify these risks to achieve acceptable risk levels.
- 5) Monitor and Review the risk: This is the step used to monitor, track and review risks.
- 6) Communicate risk status throughout project

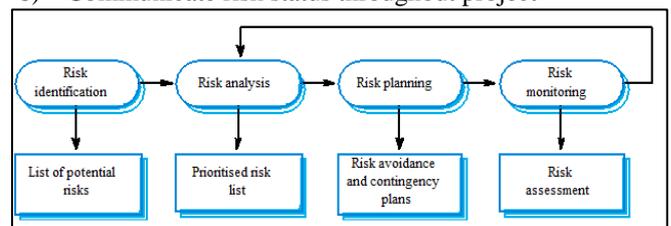


Fig. 1: Risk Management Process:

IV. RISKS CATEGORIES

Risks are identified, classified and managed before starting the actual development of a system. These risks are classified in different categories.

A. Schedule Risk

Project schedule get slip when project tasks and schedule release risks are not addressed properly.

Schedule risks mainly affect on project and finally on company economy and may lead to project failure.

Schedules often slip due to following reasons:

- Wrong time estimation
- Resources are not tracked properly. All resources like staff, systems, skills of individuals etc.
- Failure to identify complex functionalities and time required to develop those functionalities.
- Unexpected project scope expansions.

B. Budget Risk

- Wrong budget estimation
- Cost overruns
- Project scope expansion.

C. Operational Risks

Risks of loss due to improper process implementation, failed system or some external events risks.

Causes of Operational risks:

- Failure to address priority conflicts
- Failure to resolve the responsibilities
- Insufficient resources
- No proper subject training
- No resource planning
- No communication in team.

D. Technical Risks

Technical risks generally lead to failure of functionality and performance.

Causes of technical risks are:

- Continuous changing requirements
- No advanced technology available or the existing technology is in initial stages.
- Product is complex to implement.
- Difficult project modules integration.

E. Programmatic Risks

These are the external risks beyond the operational limits. These are all uncertain risks are outside the control of the program.

These external events can be:

- Running out of fund.
- Market development
- Changing customer product strategy and priority
- Government rule changes.

V. TOOLS AND TECHNIQUES FOR RISK MANAGEMENT

Risk Assessment tools are important for any software projects to be delivered successfully. It is a regulatory requirement in some organization for quality audit and compliance process. An automated Risk Assessment tools reduces audit time and findings, and a decreases risk of project failure. It improves product quality, increases

customer satisfaction, and ensures the requirements are implemented in full with compliance acceptance.

There are six major risk management process has been elaborated with its Inputs, Tools, Techniques and Outputs.

- 1) Plan Risk Management
- 2) Risk Identifications
- 3) Qualitative Risk Analysis
- 4) Quantitative Risk Analysis
- 5) Plan Risk Responses
- 6) Control Risks

A. Plan Risk Management

Risk management planning is the process of deciding how to approach and plan the risk management activities for a project. It is important to plan the risk management processes that follow to ensure that the level, type, and visibility of risk management are commensurate with both the risk and importance of the project to the organization.

| Inputs | Tools & Techniques | Outputs |
|--|--|--|
| <ul style="list-style-type: none"> - Project Management Plans - Project Charter - Stakeholders register - Environmental Factors - Organizational process assets | <ul style="list-style-type: none"> - Analytical techniques - Expert judgment - Meetings | <ul style="list-style-type: none"> - Risk Management Plan |

Table 1: Risk management planning

B. Risk Identifications

Risk Identification process determines which risks may affect the project and documenting their characteristics. It is an iterative process as risk can be identified at any levels in the project. Irrespective of risks having positive or negative consequences, all risks events and their consequences should be identified.

| Inputs | Tools & Techniques | Outputs |
|---|---|---|
| <ul style="list-style-type: none"> - Risk Management Plan - Cost management Plan - Schedule Management Plan - Quality management Plan - Human resource management Plan - Scope baseline - Activity Cost estimates - Activity Duration estimates - Stakeholder register - Project documents - Procurement documents | <ul style="list-style-type: none"> - Documentation reviews - Information gathering techniques - Checklist analysis - Assumptions analysis - Diagramming analysis - SWOT analysis - Expert judgment | <ul style="list-style-type: none"> - Risk Register |

| | | |
|---|--|--|
| <ul style="list-style-type: none"> - Enterprise environment factors - Organizational process Assets | | |
|---|--|--|

Table 2: Risk Identification process

C. Qualitative Risk Analysis

Prioritizing risks for further analysis or action by assessing and combining their probability of occurrence and impact. Qualitative risk analysis includes methods for prioritizing the identified risks for further action, such as risk response. The risk management can improve the project’s performance effectively by focusing on high priority risks.

| Inputs | Tools & Techniques | Outputs |
|---|--|---|
| <ul style="list-style-type: none"> - Risk Management Plan - Scope baselines - Risk Register - Enterprise environmental factors - Organizational process assets | <ul style="list-style-type: none"> - Risk probability and impact assessment - Probability and impact matrix - Risk data quality assessment - Risk categorization - Risk urgency assessment - Expert judgment | <ul style="list-style-type: none"> - Project document updates. |

Table 3: Qualitative Risk Analysis

D. Quantitative Risk Analysis

Numerically analyzing the effect of identified risks on overall project objectives. Quantitative risk analysis goes at least one stage further than qualitative analysis by attempting to quantify the outcome of a risk event or to attach a numerical score to the risk according to its perceived claim for preventive or mitigating action. Quantitative analysis methods attempt to assign numerical values to risks and their possible effects. They often examine the probable impact on project time and costs. Alternatively, the evaluation process can produce a ranking number for every identified risk. Ranking numbers denote the priority that a risk should claim for management attention and expenditure on preventative measures.

| Inputs | Tools & Techniques | Outputs |
|--|---|--|
| <ul style="list-style-type: none"> - Risk management plan - Cost management plan - Schedule management plan - Risk register - Enterprise environment factors - Organizational process assets | <ul style="list-style-type: none"> - Data gathering and representation techniques - Quantitative risk analysis and modeling techniques - Expert judgment | <ul style="list-style-type: none"> - Project document updates |

Table 4: Quantitative Risk Analysis

E. Plan Risk Responses

Developing options and actions to enhance opportunities and reduce threats to project objectives.

1) Plan Risk Responses Definitions

- Risk Trigger: A sign which provides warning that risk is about to occur
- Contingency Plan: Planned response to be performed when trigger happened
- Fallback Plan: Plan to be used when planned response prove ineffective
- Residual Risk: Risk remains after acceptance
- Secondary Risk: A direct result of implementing a risk response
- Workaround: Unplanned response developed to deal with occurrence of unanticipated risk events
- Contingency Reserve: Funds or time allocated by PM for known-unknowns
- Management Reserve: Funds or time allocated by top management for unknown-unknowns.

| Inputs | Tools & Techniques | Outputs |
|---|--|---|
| <ul style="list-style-type: none"> - Risk management plan - Risk register | <ul style="list-style-type: none"> - Strategies for negative risk or threats - Strategies for positive risks or opportunities - Contingent response strategy - Expert judgment | <ul style="list-style-type: none"> - Project management plan updates - Project document updates - Risk register updates. |

Table 5: Plan Risk Responses

F. Control Risks

Implementing risk response plans, tracking identified risks, monitoring residual risks, identifying new risks, and evaluating risk process effectiveness throughout the project.

1) Monitor & Control Risk

- Tracking existing risks
- Look for occurrence of risk triggers
- Monitor residual risks
- Evaluate effectiveness of risk management plan
- Collect / communicate risk status
- Determine if assumptions still valid
- Implementing risk response plans (using the Plan risk responses process)
- Recommend corrective actions
- Use contingency reserves Risk Reassessment Periodically review risk management plan and risk register and adjust them as required
- Also, close risks that are outdated
- Risk Audit Auditors should ask the project team to prove that they have identified all the risks, have plans for each major risk, and risk owner is prepared to take action.
- Evaluating risk process effectiveness continuously

| Inputs | Tools & Techniques | Outputs |
|--|--|--|
| <ul style="list-style-type: none"> - Project management plan - Risk register | <ul style="list-style-type: none"> - Risk reassessment - Risk audits - Variance and | <ul style="list-style-type: none"> - Work performance information - Change |

| | | |
|----------------------------|-------------------------------------|---|
| – Work performance data | – trend analysis | – requests |
| – Work performance reports | – Technical performance measurement | – Project management plan updates |
| | – Reserve analysis | – Project document updates |
| | – Status meetings | – Organizational process assets updates |

Table 6: Control Risks

VI. COMMONLY USED TOOLS FOR RISK MANAGEMENT IN SOFTWARE DEVELOPMENT

A. Risks Register

The risk register lists all the risks identified at the beginning and during the life of the project, their grading in terms of likelihood of occurring and seriousness of impact on the project, initial plans for mitigating each high level risk, and subsequent results.

It usually includes:

- A unique identifier for each risk
- A description of each risk and how it will affect the project
- An assessment of the likelihood it will occur and the possible seriousness/impact if it does occur (low, medium, high)
- A grading of each risk according to a risk assessment table
- An outline of proposed mitigation actions (preventative and contingency).

The register should be maintained throughout the project and will change regularly as existing risks are re-graded in the light of the effectiveness of the mitigation strategy, and new risks are identified. In smaller projects, the risk register is often used as the risk management plan.

1) Risk Identification Template

| Reference | Risk | Source (How can the risk occur) | Impact (What is the impact of the risk occurring) |
|-----------|------|---------------------------------|---|
| 1 | | | |
| 2 | | | |

Table 7: Risk Identification Template

| Ref | Description of Risk | Likelihood | Seriousness | Grade | Change | Actions | Responsible officer |
|-----|--|------------|-------------|-------|--------|---|---------------------|
| 1 | Inadequate funding to complete the project | M | M | B | NEW | Re-scope project, focusing on time and resourcing | Project Manager |
| 2 | Lack of technical skills in staff | H | H | A | ↑ | Develop training plan | Consultant |

Table 12: Control

Each risk has been rated in terms of its resulting likelihood of occurrence and the potential impact.

| Types of Risks | |
|----------------|--|
| Type | Description |
| Strategic | Related strategic mission and objectives. |
| Financial | Related to economic impact (costs, revenues, budgets). |

2) Risk register as at (date)

| |
|------------------|
| Project name: |
| Report for: |
| Project manager: |
| Project scope: |

Fig. 2: Risk register as at (date)

| Rating for likelihood and seriousness for each risk | | | |
|---|-----------------|----|--|
| L | Rated as low | E | Rated as extreme (used for seriousness only) |
| M | Rated as medium | NA | Not assessed |
| H | Rated as high | | |

Table 8: Rating for likelihood and seriousness for each risk

| Grade: Combined effect of likelihood/seriousness | | | | | |
|--|-------------|-----|--------|------|---------|
| Likelihood | Seriousness | | | | |
| | | low | medium | high | extreme |
| | low | E | D | C | A |
| | medium | D | C | B | A |
| high | C | B | A | A | |

Table 9: Grade: Combined effect of likelihood/seriousness

| Recommended actions for grades of risk | |
|--|---|
| Grade | Risk actions |
| A | Actions to reduce the likelihood and seriousness to be identified and implemented as soon as the project commences. |
| B | Actions to reduce the likelihood and seriousness to be identified and appropriate actions implemented during project execution. |
| C | Actions to reduce the likelihood and seriousness to be identified and costed for possible action if funds permit. |
| D | To be noted - no action is needed unless grading increases over time. |
| E | To be noted - no action is needed unless grading increases over time. |

Table 10: Recommended actions for grades of risk

| Change to grade since last assessment | | | |
|---------------------------------------|--------------------|---|-------------------|
| NEW | New risk | ↓ | Grading decreased |
| — | No change to grade | ↑ | Grading increased |

Table 11: Change to grade since last assessment

| | |
|-------------------------|---|
| Regulatory (Compliance) | Related to legal and contractual obligations. |
| Management | Related to decision making, resources, policies, etc. |
| Operational (Technical) | Related to delivery, support or management services. |

Table 13: Types of Risks

B. Tools for Qualitative & Quantitative Risk Management

| Qualitative Measure of Consequences of Likelihood | | | |
|---|----------------|---|-------------------------|
| Level | Description | Description | |
| A | Almost certain | Is expected to occur in most circumstances. | More than once per year |
| B | Likely | Will probably occur in most circumstances. | 1 in 1 - 3 years |
| C | Possible | Might occur at some time. | 1 in 3 - 5 years |
| D | Unlikely | Could occur at some time. | 1 in 5 - 10 years |
| E | Rare | May occur in exceptional circumstances. | 1 in 10 years |

Table 14: Qualitative Measure of Consequences of Likelihood

| Qualitative Measure of Consequences of Impact | | |
|---|---------------|--|
| Level | Description | Example detail description |
| 1 | Insignificant | Low financial loss, no risk to reputation. |
| 2 | Minor | On-site release immediately |

| | | |
|---|--------------|--|
| | | contained, medium financial loss, some customer dissatisfaction. |
| 3 | Moderate | On-site release contained with outside assistance, high financial loss and public visibility. |
| 4 | Major | Loss of capability, invocation of disaster recovery with no detrimental effects, major financial loss. |
| 5 | Catastrophic | Off-site with detrimental effect, huge financial loss. |

Table 15: Qualitative Measure of Consequences of Impact

C. Tool for Quantitative Risk Analysis

| Quantitative Measure of Consequences of Impact | | |
|--|---------------|----------------------------|
| Level | Description | Example detail description |
| 1 | Insignificant | Nil - Negligible |
| 2 | Minor | Under 50K |
| 3 | Moderate | Between \$50K - \$100K |
| 4 | Major | Between \$100K - \$200K |
| 5 | Catastrophic | Above \$200K |

Table 16: Tool for Quantitative risk analysis

| Qualitative Risk Analysis Matrix | | | | | | |
|----------------------------------|--------------------|---------------|-------|----------|-------|--------------|
| | | Impact | | | | |
| | | Insignificant | Minor | Moderate | Major | Catastrophic |
| Probability | Likelihood: | 1 | 2 | 3 | 4 | 5 |
| | A (almost certain) | H | H | E | E | E |
| | B (likely) | M | H | H | E | E |
| | C (possible) | L | M | H | E | E |
| | D (unlikely) | L | L | M | H | E |
| E (rare) | L | L | M | H | H | |

Table 17: Qualitative Risk Analysis Matrix

| Key | Description |
|-----|---|
| E | Extreme Risk: Immediate action required to mitigate the risk. |
| H | High Risk: Action should be taken to compensate for the risk. |
| M | Moderate Risk: Action should be taken to monitor the risk. |
| L | Low Risk: Routine acceptance of the risk. |

Table 18: Description

| Risks status types | |
|--------------------|---|
| Type | Description |
| Open | New item identified and awaiting action. |
| Closed | Item closed e.g. no longer a concern, rejected, etc. |
| In progress | Item undergoing code fix/mitigation activities. |
| Monitoring | Code fix/Mitigation activities complete and being monitored. |
| Resolved | Item resolved through fix/mitigation actions and resolution accepted by stakeholders. |

Table 19: Risks Status Types

VII. CONCLUSION

In this way, software risk management, risks classification, and strategies for risk management are clearly described in this paper. If risk management process is in place for each and every software development process then future problems could be minimized or completely eradicated.

Risk management is an extensive discipline, and we have given only an overview here.

The best practices or summary of managing risk on software development and software engineering projects:

- Always be forward thinking about risk management. Otherwise, the project team will be driven from one crisis to the next.
- Use checklists, and compare with similar previous projects.
- Prioritize risks, ranking each according to the severity of exposure.
- Develop a top-10 or top-20 risk list for the project.
- Vigorously watch for surfacing risks by meeting with key.
- As practicable, split larger risks into smaller, easily recognizable and readily-manageable risks.
- Strongly encourage stakeholders to think proactively and communicate about risks throughout the entire project.

Understanding various factors under risk management process and focusing on risk management strategies explained above could help in building risk free products in future.

REFERENCES

- [1] Hall, E. (1998): Managing Risk: Methods for Software System Development, Addison-Wesley, New York.
- [2] Jones, C. (1994): Assessment and Control of Software Risk, Prentice-Hall, New York.

- [3] Karolak, W. (1995): *Software Engineering Risk Management*, Wiley-IEEE Press, San Francisco.
- [4] Charette, R. (1989): *Software Engineering Risk Analysis and Management*, McGraw Hill, New York.
- [5] Boehm, B. (1989). *Software Risk Management*. Washington, DC, IEEE Computer Society Press.
- [6] Boehm, B. (January 1991). "Software Risk Management: Principles and Practices." *IEEE Software*: 32-41.
- [7] Risk Factors in Software Development Phases, Haneen Hijazi, ShihadehAlqrainy, Hasan Muaidi & Thair Khdour.
- [8] A Proposed Taxonomy for Software Development Risks for High-Performance Computing Scientific /Engineering, Richard P. Kendall, Douglass E. Post, Jeffrey C. Carver, Dale B. Henderson & David A. Fisher.
- [9] Abdullah, T., Mateen, A., Sattar, A., & Mustafa, T. (2010). Risk analysis of various phases of software development models. *European Journal of Scientific Research*, 40(3), 369–376.
- [10] Arshad, N., Mohamed, A., & Nor, Z. (2007). Risk factors in software development projects proceedings of 6th WSEAS International Conference on Software Engineering, Parallel and Distributed Systems, pages 51–56, 2007.
- [11] B. W. Boehm, "Software Risk Management Principles and Practices", *IEEE Software*, vol. 8, no. 1, (1991).
- [12] P. L. Bannerman, "Risk and Risk Management in Software Projects: A reassessment", *Journal of Systems and Software*, vol. 81, no. 12, (2008), pp. 2118-2133.
- [13] Evolving a New Software Development Life Cycle Model SDLC-2013 with Client Satisfaction by Naresh Kumar, A. S. Zadgaonkar, Abhinav Shukla. *International Journal of Soft Computing and Engineering (IJSCE)* ISSN: 2231-2307, Volume-3, Issue-1, March 2013.
- [14] Risk Assessment of Information Technology Systems by direktor@vtsns.edu.rs; ljaga@eunet.rs.
- [15] Risk Assessment Handbook www.nationalarchives.gov.uk/dc-guidance Risk Management by Laurie Williams.
- [16] *Software Risk Management: Importance and Practices* Abdullah Al Murad Chowdhury and Shamsul Arefeen.
- [17] *Software Risk Analysis and Management* by BojanCukicBojanCukic1.304.293.0405.
- [18] *Software Risk Management* by Linda Westfall The Westfall Teamwestfall@idt.net.
- [19] Case Study on E-Business V Corp. Software Project Risk Management with Interpretive Structural Modeling, Jiangping Wan, Zhong Wang School of Business Administration, South China University of Technology, Guangzhou, China -published 27 March 2015.
- [20] *Software Development Risk Aspects and Success Frequency on Spiral and Agile Model* by M. Soumya Krishnan published on 1 January 2015.
- [21] Prediction of risk factors of software development project by using multiple logistic regression by thitima christiansen 1, pongpisit wuttidittachotti 1, somchai prakancharoen 2 and sakda arj-ong vallipakorn published on February 2015.