

Produced by
STeP-IN
Forum

STeP-IN SUMMIT 2008

Hosted by



5th International Conference on
Software Testing

Risk Identification - First Step for Managing Risks in Testing Projects

Vidya Viswanath &
Sundaresa Subramanian G

PEVS - Infosys Technologies Ltd

vidya_v@infosys.com & ssubramanian_gv@infosys.com

Copyright: STeP-IN Forum and Quality Solutions for Information Technology Pvt. Ltd.

Published with permission for restricted use in STeP-IN SUMMIT 2008 in agreement with full copyrights from owner(s) / author(s) of material. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior consent of the owner(s) / author(s). This edition is manufactured in India and is authorized for distribution only during STeP-IN SUMMIT 2008 as per the applicable conditions.

Practices Experience Knowledge Automation

Win in the flat world

Risk Identification – First Step for Managing Risks in Testing Projects

Vidya Viswanath - Senior Test Manager
Sundaresa Subramanian G- Test Manager
PEVS – Infosys Technologies Ltd

Topics Covered

- Introduction
- Definitions
- IMMUNE Framework
- Components of IMMUNE Framework
- Implementing IMMUNE Framework
- Benefits
- Conclusion
- Q & A

Infosys2Win in the flat world

Introduction

- “*Heisenberg’s Uncertainty Principle*” states that if one parameter is measured accurately then the other parameter becomes less accurate.
- *Uncertainty* in IT field directly relates to *Risks* that are faced in a project. Focus is on *identifying* more risks to make the project parameters become more *predictable*.
- If a risk is not identified, it cannot be evaluated and managed.
- Managers track and mitigate Risks in various ways. A key element of uncertainty and risk is to *define the most appropriate decision criterion*

Definition of Risk

Risk is the possibility that an organization will **NOT**:

- Achieve its goals
- Operate effectively and efficiently
- Protect itself from loss
- Provide reliable financial data (reports)
- Comply with applicable laws/regulations
- Comply with defined policies/procedures

Risk Identification is iterative ...

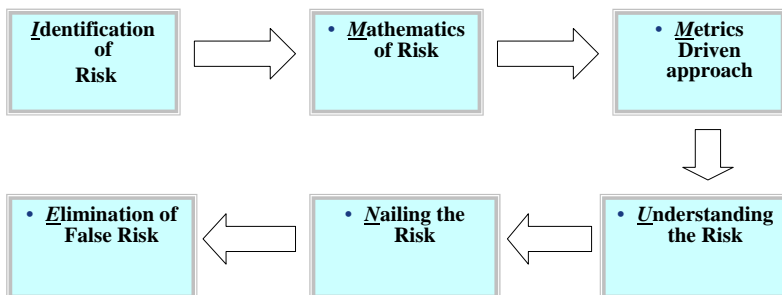
Risk Management starts with effective Risk Identification ...

IMMUNE Framework

- Identification of Risks- The Philosophy behind it
- **M**athematics and **M**etrics based Approach to Risk Identification
- **U**nderstanding and Defining Risks Correctly
- **N**ailing the Risk –Impact, Severity and other factors
- **E**limination of False Risks

Let's define a framework for Risk Identification ...

Suggested Framework Diagram



I - Identification of Risks- The Philosophy behind ...

- Risk is a possibility, not the certainty, of suffering a loss
- Successful teams deal with risk by recognizing and minimizing uncertainty
- A successful risk identification system includes education and communication to stakeholders involved in pivotal project roles
- Teach key project team members to identify risks – They are the people who are at ground level
- Risk Identification is a continuous process over the duration of Software Testing Life Cycle

Identification of Risks – Continued...

Phase	Activities to identify Risks	Types of Risks
Req. Analysis (Technical Risk Occurrence)	<ul style="list-style-type: none"> • Kick off meeting with Stakeholders • Clarifications 	Technology, Skill set, Project Size, Schedule, Functionality, Standards etc.,
Test Approach (Management and Legal Risk Occurrence)	<ul style="list-style-type: none"> • Meetings • Estimations • Regulatory Discussions • Dev Scheduling etc., 	Changing requirements, Govt.Regulations, Warranty, Non-availability of signed off documents, collaterals etc.,
Test Planning (Technical Risk Occurrence)	<ul style="list-style-type: none"> • Change Management • Preparation of test ware 	Training issues, teething issues, Lack of clarity on test criteria, scope creep
Test Management (High Occurrence of Personnel Risk)	<ul style="list-style-type: none"> • Test Execution/ Status Reporting • Defect Management 	Late code delivery, Inadequacy in everything, Staff issues, Lack of Planning... THE LIST IS HUGE

Mathematics & Metrics based Risk Identification

Parameters/Metrics	Remarks
Estimated Cost Impact (RECI)	Calculated Cost Impact due to the Risk Occurrence
Actual Cost Impact (RACI)	Actual Cost Impact incurred after Risk Occurrence
Estimated Schedule Impact (RESI)	Estimated Schedule Impact due to occurrence of Risk
Actual Schedule Impact (RASI)	Actual Impact on Schedule because of the occurrence of Risk
Risk-Cost Deviation (RCD) in %	$(RECI - RACI) / RECI * 100$
Risk-Schedule Deviation (RSD)	$(Estimated\ Schedule\ Impact - Actual\ Schedule\ Impact) * 100 / (Estimated\ Schedule\ Impact)$

Primary focus should be to avoid/minimize RCD and RSD ...

U - Understanding and Defining Risks Correctly

Generic:

- How could you fail?
- What can go wrong?
- What must go right for us to succeed?
- When, where, why, how are the risks likely to occur?
- Where is your greatest exposure?
- What is the source of each risk?
- What are the consequences of each risk?

Financial & Legal

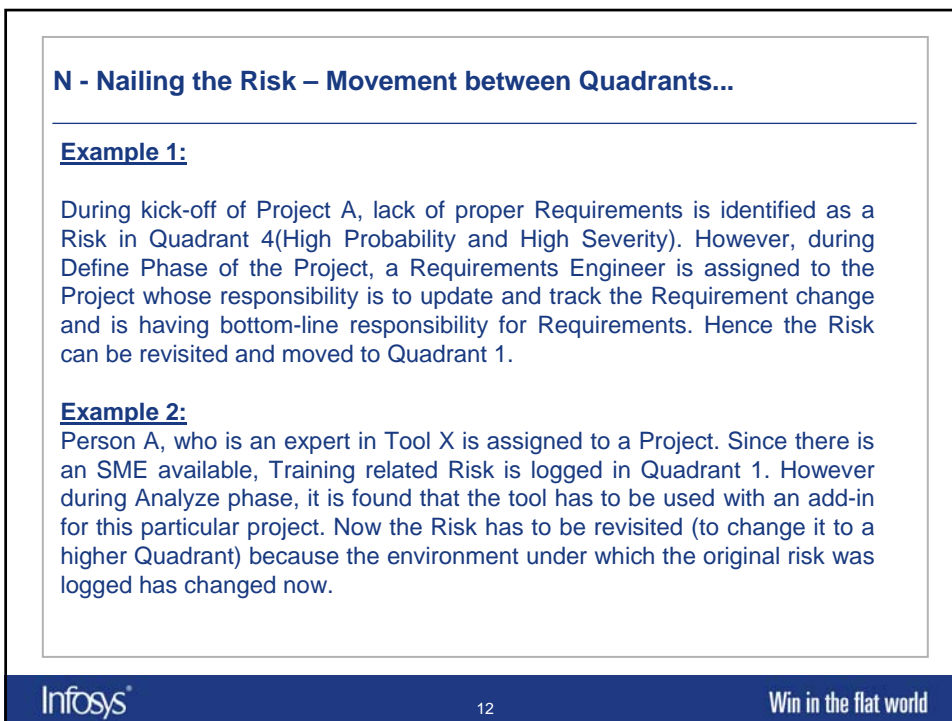
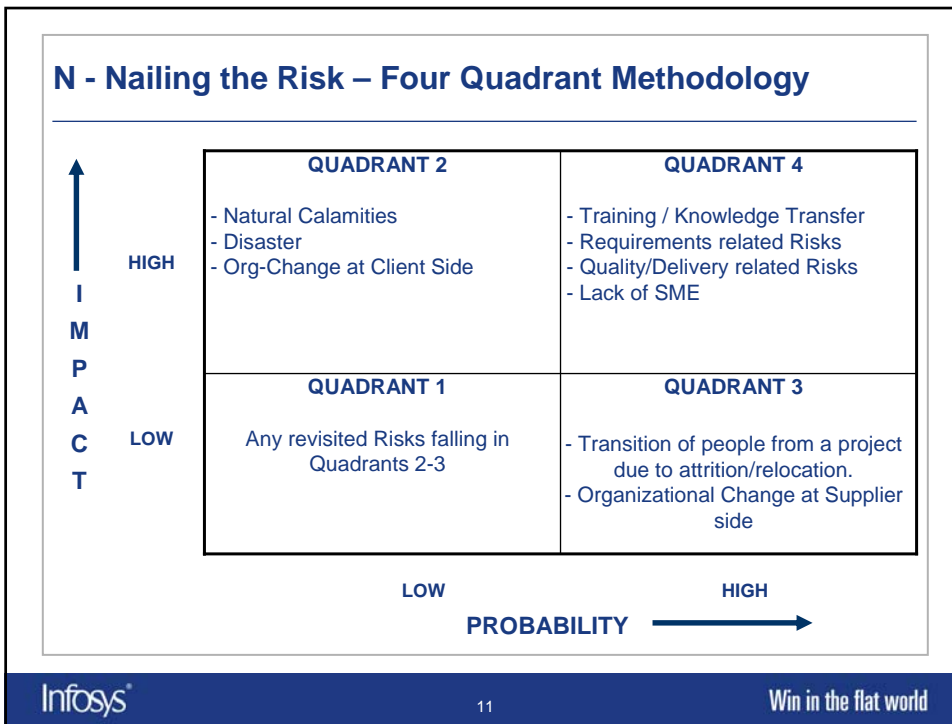
- How do you bill and collect your revenue?
- How often might these risks occur?
- On what do you spend the most money?
- What assets do you need to protect?
- What is the potential cost in time, money and resources?
- What activities are regulated?
- Are we following the required Security & Compliance standards as mentioned by Client in handling their data?

Technical:

- Are all the base documents available and signed off?
- How can someone bypass the internal controls?
- What types of transactions in this project provide the most risk?
- Where are you most vulnerable?
- On what concept of this project do you lose your sleep over?

Management:

- Do you have "liquid" assets or assets which have alternative uses - read "assets" as "resources"?
- How reliable is the information?
- Is there a need to research specific risks or seek further information?
- On what information do you most rely?
- What are the accountability mechanisms - internal and external?
- What controls presently exist to mitigate the risk?
- What decisions require the most judgment?
- Who might be involved?
- Who are the stakeholders?



Elimination of False Risks

Scenario 1:

A and B are handling 2 different projects in the same sub-domain. B is relatively new to the Project.

A handles a Project which is NOT a sweet spot and the Project handled by B is the Primary Sweet Spot.

Most of the Risks in the Project handled by A are focused towards Training and Knowledge Level of the Project Resources.

B incorporates all the Risks found by A without analyzing its applicability to his/her current project.

When the Risk Register is shared with the Client, they have serious questions about the Knowledge Level of Resources in the Project. The Client puts the Project ON HOLD and escalate to the Engagement Team.

Elimination of False Risks...continued...

Scenario 2:

C is handling the proposal for a 5 member Automation testing project.

The client had clearly stated the requirements and had assured that 3 licenses for Automation Tool would be made available.

C during Risk Identification lists down lack of 2 more licenses as a major risk affecting the Project Delivery.

The quote reaches the client and they decide to proceed with a competitor who gave the option of working in shifts with the available 3 licenses.

Sometimes False Risks can be as lethal as Real Risks...

Implementing IMMUNE Framework

- **STEP 1: Collecting Risk related data**

- Select a Group/Account and start collecting Risk related data
- Circulating Questionnaire among the group to collect Risk data

- **STEP 2: Analyzing the Collected Data**

- Brain storm to find out common pattern and differences in data

- **STEP 3: Apply Calculations to form a Baseline**

- Apply calculations to aid the formation of a repository for Risk Data

Data collection frequency – Every Quarter

As more and more data is collected, the baseline moves towards accuracy ...

Advantages of IMMUNE

- Gives better Understanding of the various dimensions of Risk Identification.
- Understand how a structured Risk Identification Process can improve the predictability of the testing project.
- Results in Reduced Cost Variance because of identification of Risks
- Improves Employee Morale – because of increased predictability of the Project thereby reducing working extended hours
- Helps in optimization of utilization of resources by matching their skills and capabilities
- As a process could be reused across the Organization

**IMMUNE works based on the assumption that a proper data collection mechanism and process is already in place.
Accurate Data Collection is the Key for this framework to be effective ...**

CONCLUSION

- Once risks are identified, they can be eliminated, mitigated or transferred.
- IMMUNE allows a consistent and repeatable expertise-driven approach to risk identification.
- From this, the basis for measurement and common metrics emerges.
- Successful use of IMMUNE framework depends on continuous identification and storage of risk information as it changes over time.
- Descriptions or measurements of the corresponding business risks mitigated can be used to clearly demonstrate the business value of the software risk identification framework.

Infosys®

17

Win in the flat world

Infosys®

Win in the flat world

Questions?

