IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

Advance Tools and Techniques for Software Risk Management

Satwik Kumar B Shiri[1], Sanam Satya Krishna Teja[2], Nithya Ganesan[3]

B.E Student, Department of Computer Science, RVCE, Bangalore, India[1,2]

Assistant Professor, Department of Computer Science, RVCE, Bangalore, India[3]

Abstract: Software development process nowadays faces many challenges and risks. Software tools have been used in software development for a long time now. They are used for performance analysis, testing and verification, debugging and building applications. Software tools can be very simple and lightweight, e.g. linkers, or very large and complex, e.g. computer-assisted software engineering (CASE) tools and integrated development environments (IDEs). Some aspects of software development, like risk management, are done throughout the whole project from inception to commissioning. In order to manage the risks we need to understand the scope and objectives of the software developments and use the appropriate risk management tools and techniques. The aim of this research paper is to demonstrate the advanced tools and techniques used for software risk management.

Keywords: Software development, Software risks, Risk management, Risk management tools, Risk assessment, Software engineering tools.

I. INTRODUCTION

There are many risks involved in creating high quality software that need to be carefully managed. Despite of having new technology, innovative methods and tools, development process is still full of risks. In the article by Michael Bloch, Sven Blumberg, and Jürgen Laartz in October 2012, according to the research conducted by McKinsey & Company in collaboration with the University of Oxford on average, large software related IT projects (with budget>$15 million in 2010 dollars) run 66 percent over budget and 33 percent over time, while delivering 17 percent less value than predicted. Therefore, to make sure that project is successful we require managing specific IT risks related to our software projects: risk identification and storing it in a shared data storage, assess risks, using tools and techniques, choose appropriate mitigation action and track that mitigated risks are lower than they were. The need for project risk management has been widely recognized by all software development companies such as Amazon, Microsoft, Oracle, IBM etc.

The science of risk management was developed back in the sixteenth century during the Renaissance, a period of discovery, but regarding the subject of Risk Management Process (RMP), since 1990 a large number of methodologies and methods have been generated to address the need for more effective risk management [7]. Among them we can distinguish the PUMA [5] and the MRMP [8] in construction engineering context; the RFRM [6] in system engineering context; the SHAMPU [2] and the PMBoK [9] in project management context; the standard of the AS/NZS 4360 [4] and the DoD [3] in public application context, etc. In this paper, we have investigated and compared most of risk related topics in software engineering context.

II. CONSIDERATIONS

The value of software tool is increased if there are software checklists available. Some tools have predefined risk categories as not all identified risks should be treated the same. Some identified risks are likely to occur, and some, if realized, would have a bigger impact. Risk analysis and management depends on the types of risks being considered.[13]

A. *Technical risks*

Risks that are associated with the performance of the software product and include problems with languages, project size, project functionality, platforms, methods, quality, reliability and timeliness issues. Even if there are no mid-project changes in scope, unforeseen technical complications can also turn the project upside down. Project managers might know the technologies they are using in the project very well but when they integrate it with another component, it's a complete mess.

B. *Financial risks*

These risks include cash flow, capital and budgetary issues, and return on investment constraints. These risks are associated with the cost of the software product during software development, including its final delivery, which includes the following issues: budget, nonrecurring costs, recurring costs, fixed costs, variable costs, profit/loss margin, and realism.

C. *Personnel risks*

Risks include staffing lags, experience and training problems, ethical and moral issues, staff conflicts, and productivity issues. Other resource risks include unavailability or late delivery of equipment & supplies, inadequate tools, inadequate facilities, distributed locations, unavailability of computer resources, and slow response times.

D. *Schedule and scope risks*
These risks are associated with the schedule and scope of the software product during development. Changes in scope are frequent in IT projects and to some extent they are quite logical.

III. ANALYSIS OF SOFTWARE RISK MANAGEMENT

Risk identification and risk assessment should be done as early as possible to minimize negative deviations and to maximize positive results during project development. Assessing software risks means determining the effects of potential risks. For the purposes of risk assessment the automated tool might provide predefined set of criteria that would help the experts to conduct evaluation.

Several approaches to software risk management have since been proposed and used in the software engineering context. However, despite of several studies and experiences published about risk management, the software industry, in a general way, does not seem to follow a model to analyze and control the risks through the development of their products [11]. According to Johnson [10] two approaches to software project management can be identified, traditional and risk-oriented. The traditional approach is reactive in nature and deals with problems generic to all software projects systemically and project specific problems as they arise. The later approach, however, is proactive as it seeks to Identify and manage unique aspects of a specific project before they impact the project.

Risk analysis and management are usually based on the information collected from traditional knowledge, or similar well-known cases, common sense, results of experiments or tests, reviewing of inadvertent exposure. The first thing for the automated tools is to collect historical data to build up a database. Once the database exists, it will process the data and mine some useful information to help the manager analyze risks and make decisions. Today's tools can automatically store all project results in a central repository shared by all users. Requirements and changes can be edited, specified and prioritized. Tasks are derived from requirements, which can be traceable through the entire life cycle. This means that *data storage and analysis* should be an important criterion when choosing the system. Today we have a great choice of different technologies and may use software as we need. Many software users prefer computer tools with much lower setup time. They want to forget about installation, implementation, training and maintenance efforts. Today, the value is not defined as much by functionality anymore but by connectivity. The user seems to move from process focus and client server architecture to distributed functions and data centric software with real-time connectivity.

Supporting guidance, standards, and risk methodologies would help users solve on the scientific basis the following practical issues in the system life cycle: analysis of quality management systems for enterprises, substantiation of quantitative system requirements to hardware, software, users, staff, technologies; requirements analysis, the evaluation of project engineering decisions, investigation of problems concerning potential threats to system operation including information security and protection against terrorists; evaluation of system operation quality, substantiation of recommendations for rational system use and optimization.[1]

Sometimes, in environments where risk assessments are performed but are not standardized, risk evaluations may vary from one assessor to the next. Whether an appropriate action is taken depends on the particular assessor, meaning that similar issues may end up being treated differently. To avoid inconsistent risk assessments a single system should be used to collect and manage risk management related activities. The system should guarantee that corporate risk tolerance thresholds are employed and followed for risk-related activities across the whole IT project.

PMBOK [9] , by the Project Management Institute (PMI), is a project management guide, and an internationally recognized standard, that provides the fundamentals of project management as they apply to a wide range of projects, including construction, software, engineering, automotive, etc. According to this guide, risk management comprises a number of processes which are :

- Risk Management Planning
- Risk Identification
- Qualitative Risk Analysis
- Quantitative Risk Analysis
- Risk Response Planning
- Risk Monitoring and Control

Risk Management Planning
- deliverable is the Risk Management Plan

Risk Identification
Risk categories:
- technical
- project management
- organizational
- external

Qualitative Risk Analysis
- define probability and consequences
- data gathering
- impact by objective
- assumptions testing
- data precision ranking

Quantitative Risk Analysis
- individual and project risk
- probability distributions
- sensitivity and decision tree analysis
- simulation methods

Risk Response Planning
Responses should be:
- appropriate
- cost effective
- timely, realistic
- agreed (funded)

DOI 10.17148/IJARCCE.2016.53110

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

Risk Monitoring and Control

- ongoing, continuous action
- risks monitored
- new risks identified
- effectiveness of risk management evaluated

IV. AVAILABLE TOOLS AND TECHNIQUES

In order to offer high-quality software products to the market on time and as per the market's requirements, it is important to find computer-based tools with high accuracy probability to help managers make their decision. Software risk analysis and management can be partially transferred into data analysis or data mining. Automated tools are designed to assist project managers in planning and setting up projects, assigning resources to tasks, tracking progress, managing budgets, requirements, changes and risks as well as analyzing workloads. To provide more effective ways of risk management, software tools, which are intelligent and adaptive to risk management strategies, are needed.

4.1 Active Risk Manager

Active Risk Manager (ARM) is the world's leading Enterprise Risk Management (ERM) software package. Unlike traditional, compliance-focused "GRC" solutions, ARM delivers far more value and capability to its users. With its robust and unique integrated approach, ARM is the only ERM solution that addresses the risk management needs of the entire organization. From managing project and program risk through to strategic business planning, ARM helps organizations identify, analyze, control, monitor, mitigate and report on risk across the enterprise.

ARM is the award-winning core powering ERM in some of the world's most respected organizations including London Underground, Crossrail, Lockheed Martin, EADS, US Department of Homeland Security, UK MOD, Saudi Aramco, Rio Tinto, Bechtel and Skanska. Combined with the full solution portfolio including ARM Risk Performance Manager, ARM Risk Connectivity, ARM Apps and ARM Unplugged, ARM offers a complete ERM solution with modules that add value to and increase the effectiveness of risk management within your organization.

4.2 RiskWatch

Since 1993, RiskWatch has been a global leader in providing risk assessment solutions. RiskWatch believes that you can't manage security and compliance risk effectively if you can't measure it.

- A comprehensive framework that is evidence- based and follows the risk models promulgated by ISO 32001, Sandia Lab and FEMA.
- A framework that can be easily customized by the customer to perform any of type of risk assessment that is relevant to their industry.
- An enterprise model that provides our customer with a single view of risks across the distributed enterprise.
- Protection based on a real-time risk score to focus efforts and maximize results.
- A technology agnostic solution that is designed to support variety of ecosystems.
- Cutting edge information and intelligence against the emerging threats and vulnerabilities.
- A content library with thousands of U.S. and International regulations, best practices and case studies.

4.3 Risk+

Risk+ is a comprehensive risk analysis tool that integrates seamlessly with Microsoft Project to quantify the cost and schedule uncertainty associated with your project plans. Precisely predicting how long a project will take or how much it will cost is almost impossible, and single point estimates for task duration and costs can be dangerously misleading. Risk+ uses sophisticated Monte Carlo-based simulation techniques to answer questions such as: "What are the chances of completing by 2/28/2002?" or "How confident are we that costs will be below $9 million?" Expensive scheduling systems have provided these tools for years. Now Risk+ brings this power to your PC at an affordable price.

4.4 ClearRisk

ClearRisk is based in St. John's NL, and has worked very hard to be a leading provider of web-based risk and claims solutions since 2006. ClearRisk was conceptualized and is led by Craig Rowe, who has been in the risk and insurance industry since 1989. From his professional experience; his extensive work in industry associations such as the Risk and Insurance Management Society (RIMS); and as a writer and presenter throughout North America on risk management, Craig developed an approach to talking about risk that business people relate to. "There's nothing mystical about risk management. It involves formalizing best practices that businesses already employ but don't think of as risk management."

ClearRisk exists to provide enterprise quality claims and risk solutions at mid-market prices. Our solutions allow our customers to organize, automate and analyse their risk, insurance and claims data. ClearRisk's solutions enable our customers to manage their claims and risk better, easier and more cost effectively. Companies and organizations should be able to access world class solutions using the most modern technologies. They should expect to get everything they need without paying for the things they don't need. ClearRisk solutions are constantly evolving with our customers. As a web-based solutions provider, our customers are always using the latest version. We add features, improvements and functionality regularly, so the changes are iterative and not disruptive to users.

The scope of the Risk IT framework is also fully covered within the scope of the COBIT 5 framework. Risk IT provides an end-to-end, comprehensive view of all risks related to the use of IT and a similarly thorough treatment of risk management, from the tone and culture at the top, to operational issues. *Risk is a natural part of the business landscape. If left unmanaged, the uncertainty can spread like weeds. If managed effectively, losses can be avoided*

DOI 10.17148/IJARCCE.2016.53110

and benefits obtained. In business today, risk plays a critical role. Almost every business decision requires executives and managers to balance risk and reward. Effectively managing the business risks is essential to an enterprise's success. Too often, IT risk (business risk related to the use of IT) is overlooked. Other business risks, such as market risks, credit risk and operational risks have long been incorporated into the corporate decision-making processes. IT risk has been relegated to technical specialists outside the boardroom, despite falling under the same 'umbrella' risk category as other business risks: failure to achieve strategic objectives.

Risk IT is a framework based on a set of guiding principles for effective management of IT risk. The framework complements COBIT, a comprehensive framework for the governance and control of business-driven, IT-based solutions and services. While COBIT provides a set of controls to mitigate IT risk, Risk IT provides a framework for enterprises to identify, govern and manage IT risk. Simply put, COBIT provides the *means* of risk management; Risk IT provides the *ends*. Enterprises who have adopted (or are planning to adopt) COBIT as their IT governance framework can use Risk IT to enhance risk management.

4.5 Risk Radar Enterprise (RRE)

Risk Radar Enterprise provides very good functionality at the Enterprise, Program, and/or Project levels when implementing a Risk Management Program. The application framework grows with your risk management program maturity and requirements. Risk Radar Enterprise empowers managers and provides their teams the visibility they require to proactively Identify, Analyze, Track, Control, Mitigate and Report Risk/Opportunities**.** It enables cost effective management and communications of Cost, Schedule, Technical/Performance risks/opportunities within a common flexible and scalable enterprise framework. It increases the visibility of program risks by helping them identify, analyze, track, mitigate, and control them. That translates into huge amounts of money and man-hours saved – as well as projects being delivered on-time and on-budget.

4.6 JCAD's CORE

JCAD's web-based enterprise risk management software, CORE provides businesses with a framework that enables the controlled management of risk and compliance with a clear link to objectives, strategy and projects. It has been designed to simplify the risk management process in both the public and commercial sectors. This intuitive and flexible risk management software is completely scalable and allows your organization to easily establish and maintain a comprehensive and effective risk management system.

Unlike many alternatives on the market, JCAD's Risk Management System CORE is not overly complex and is easily configurable. This flexibility means that it will align perfectly to your existing Enterprise Risk Management (ERM) framework. It also brings together a range of additional features and benefits such as opportunity management, compliance and audit tracking, to provide you with a complete business assurance and risk management solution.

V. CONCLUSION

This paper has given the description of the advance tools for risk management in software engineering. Risk Management is very important aspect of software development. In every phase of the software development the project is assessed for the risks. The complexity of risk management increases with the complexity of the developed system. The risk management tools which are intelligent and automated are widely used. Such tools have the capacity to be used with any development methodology, whether traditional, agile, or even a combination of them. There is no good or bad tool for risk management as the field is still under research and many new tools are being released to the market daily. One can make use of the tools according to the need of the project.

REFERENCES

[1] Avdoshin S., Pesotskaya E., Business informatization. Managing risks, Moscow: DMK Press, 2011, 176 p. [in Russian].
[2] Chapman C.B., Ward, S.C. Project Risk Management, Processes, Techniques and Insights, 2nd Edition. John Wiley. Chichester, UK. 2003.
[3] Conrow E.H. Effective Risk Management: Some Keys Success, 2nd Edition. American Institute of Aeronautics and Astronautics. Reston, USA. 2003.
[4] Cooper D. Tutorial Notes: The Australian and New Zealand Standard on Risk Management (AS/NZS 460). Retrieved: may 2004 from http://www.broadleaf.com.
[5] Del Cano A., De La Cruz M.P. Integrated methodology for project risk management. Journal of Construction Engineering and Management. 2002, 128(6): 473-485.
[6] 6. Haimes Y.Y., Kaplan S., Lambert J.H. Risk filtering, ranking and management framework using hierarchical holographic modeling. Risk Analysis. 2002, 22(2): 381-395.
[7] Kwak Y.A. Stoddard J. Project risk management: lessons learned from software development environment. Technovation, 2003, 24: 915-920.
[8] Pipattanapiwong, J. Development of Multi-party Risk and Uncertainty Management Process for An Infrastructure Project. PhD Thesis, Kochi University of Technology. Kochi, Japan. 2004.
[9] PMI (Project Management Institute). A Guide to the Project Management Body of Knowledge (PMBoK). Newtown Square. Pennsylvania, USA. 2004.
[10] Johnson D. L., Risk Management and the Small Software Project, viewed 4 May 2009 http://www.sei.cmu.edu/iprc/sepg2006/johnson.pdf
[11] Kimer, T.G., &Concalves, L.E., 2006, Software Engineering Techniques: Design for Quality , IFIP International Federation for Information Processing, Volume 227, pp. 149-154.
[12] Software Risk Management: Using Automated Tools, Sergey M. Avdoshin, Elena Y.Pesotskaya School of Software Engineering, Software Management Department, National Research University Higher School of Economics, Moscow, Russian Federation.

DOI 10.17148/IJARCCE.2016.53110