Volume 4, Issue 3, March 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Framework to Reduce the Project Related Risk

Shweta Sankhwar, Dhirendra Pandey*
Department of Information Technology,
Babasaheb Bhimrao Ambedkar University, Lucknow, India

Abstract—Software risk is a condition that can result failure of software project and loss in terms of cost and quality. There is no doubt that security is now a 'vibrant burning issue'. It is observed that finding and fixing a software risk after delivery is often more expensive than finding and fixing it during Software Development Life Cycle (SDLC).It needs to address prominently and no escape way is feasible. The failure and success of any software depends upon the proper management of risk. There may be possibility of Project Related Risk (PRR) which may jeopardize the software project i.e., loss of physical security, loss of authentication, loss of access control, loss of confidentiality. An exhaustive review on software risk management revealed the fact that there is no standard framework or methodology available to reduce software project related risk. Therefore, an effective framework is developed for quality software project which may be able to overcome the aforesaid software project related risk (PRR). The PRR could be pondered to reduce threats and vulnerabilities through proposed framework. It consists of three phases and used to manage PRR: identifying risk factors, analyzing risk probabilities and its effects on software quality, risk mitigation, and risk monitoring. Furthermore, some future research directions are discussed to enhance the software project quality and to achieve the objectives emphasizing on software related risk reduction.

Keywords—Software risk, software risk management, risk, associated with physical, authentication, access control, audit, and confidentiality.

I. INTRODUCTION

Risk is an essential factor for the quality software development and at the same time project may be unsuccessful by its impact. The impact of risk on software project may result in poor quality software project and possibility of suffering loss. Risk defines uncertainty and loss of software project. Risk may be defined as dynamic risk and static risk. Dynamic risk is concerned with the profit or loss of organisational assets, whereas, static risk may provide only loss of the organisational assets. Software risk can be divided into two parts i.e. internal and external [1]. Internal risks are those risks which arise from the risk factors within the organization whereas; external risks are vice-versa. Internal risk is divided into three categories i.e., product, process and project. Product risks are technical risk, pending faults and possible shortcomings. Process risk can be the resultant or outcome of product risk. Project risk concerns the performance of the project. [1, 2]

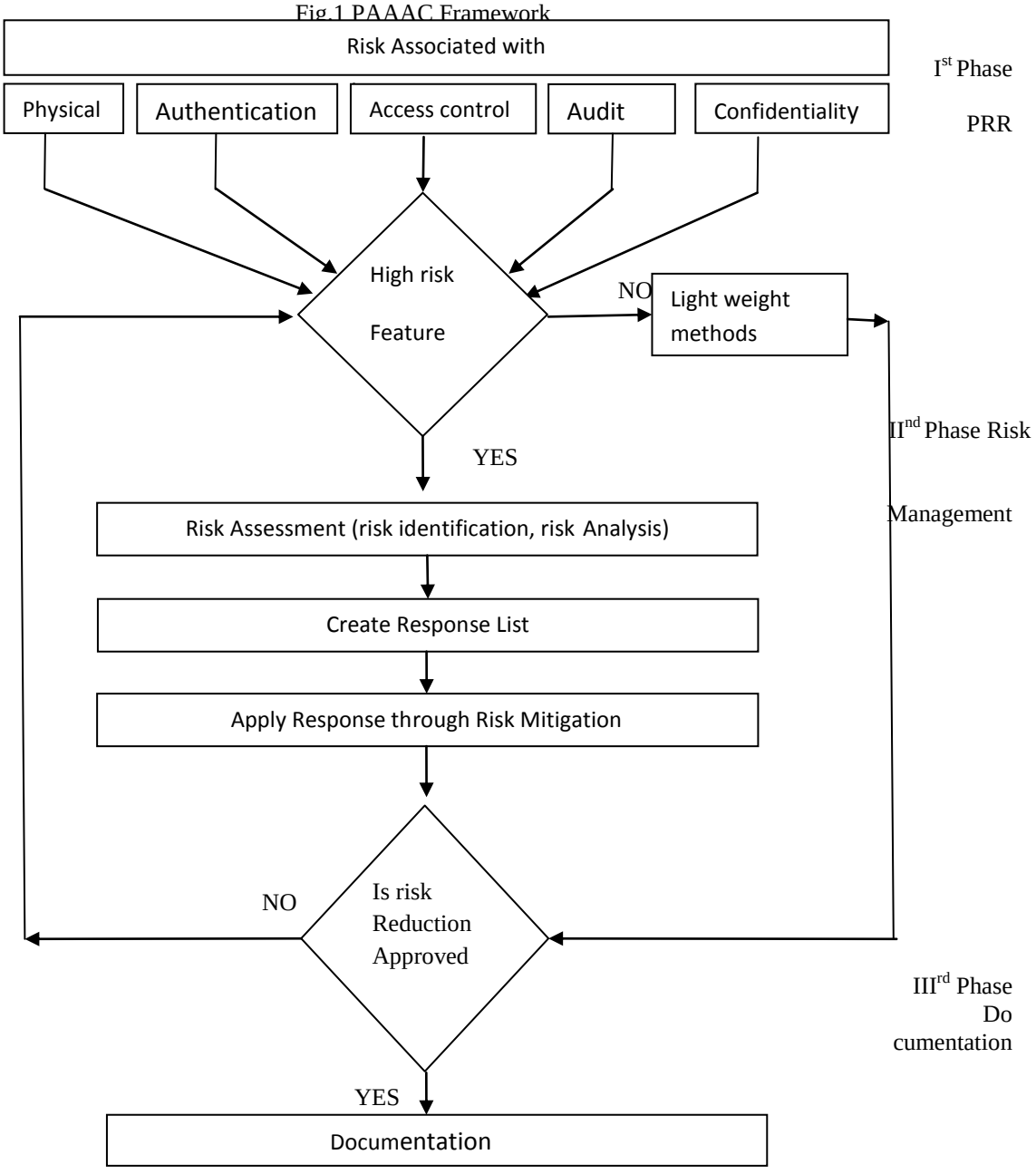
The Project related risk (PRR) may spawn loss of physical security, loss of authentication, loss of access control, loss of audit, and loss of confidentiality. Security features like cryptography, strong authentication and access control plays a critical role in software security. Security carries the concept of safety, confidentiality and reliability. Number of security loopholes and vulnerabilities exists due to the defects. Threats take advantage of project weaknesses or vulnerabilities, which leads to harm on reliability, confidentiality, integrity, availability, no repudiation as well as other features of software security. Risk is considered as potential problem, which may occur and create the major problem in software project. Therefore, Integration of security features must be a part of software development life cycle and it is necessary to analyse and manage the risk factors [3]. Effective risk management i.e., risk assessment and risk mitigation both is significant for the success of software development. As a result, an attempt has been made to propose a framework to reduce project related risk (PRR). The main objective of the presented article is to emphasize on project related risk framework which is based on technique to reduce the project risk and develop the secure software project. The organisation of this paper is as follows: Section-2 presents the proposed framework and their details, section-3 presents the discussion, and section-4 presents the future direction of software project related risk issues. The concluding remarks are discussed in section-5.

II.THE FRAMEWORK

Security refers to the protection of software products from unauthorized access, alteration and destruction. Therefore, security requirement is presently a major concern of software project and it is generally recommended to take care of security prior to software development process. [4] In this paper, we have proposed an effective PAAAC (Physical, Authentication, Access, Audit, and Confidentiality) framework shown in Fig.1. This framework is concerned with identifying and reducing security risks .The goal of the Framework is to provide high level of software project protection against disclosure, alteration, destruction etc to attain the confidentiality, integrity, availability and some other security aspects. The proposed framework is more effective to produce software quality. There are three phases of framework. In

first phase it covers few dimensions of software risk, called software project related risk (PRR) i.e., loss of physical security, loss of authentication, loss of access control, loss of confidentiality. Second phase of framework is risk management which is one of the most important aspects of security. There are some controls available which are used to reduce the risk i.e., risk assessment and risk mitigation. These controls can be useful for finding cause of risk and also it help to reduce the risk. These risks are analyzed based on their criticality and likelihood, and a decision is made whether to mitigate the threat or accept the risk associated with it. During SDLC, risk assessment and risk mitigation are accomplished to make software more effective and efficient. Risk assessment and risk mitigation reduce the reason responsible for the unsecure software project. Risk assessment determines the existence of risk whereas risk mitigation minimizes the PRR. PRR are examined for level of risk feature i.e. high and low. The PRR which have low risk feature are moved for light weighted method for risk reduction. And the PRR having high risk feature are moved for risk assessment where risk identification and analysis is done to create identified list or response list. These identified risks are removed through the risk mitigation method and if the risk reduction is approved then the documentation is done else whole process is iterated which is the last phase of framework.

Fig.1 PAAAC Framework



The aim of the research is to provide the solution of aforesaid problem i.e., project related risk. Internal threats such as installation or use of unauthorized hardware, peripherals; abuse of computer, access controls, physical theft of hardware or software; human mistake; damage by displeased, use of organization resources for illegal communications or activities and installation or use of unauthorized software.[5] Few threat or risk i.e., project related risk are defined below:

A. First Phase of Framework

1) Loss of Physical Security

Information of a sensitive variety where unauthorized access occurs may lead to considerable damage for software project.

1. The physical access to the servers, switches, routers, cables and other devices in server room can do enormous damage.
2. Intruder could break in, or someone who has authorized access could misuse the authority.
3. Hackers can use any unsecured computer that's connected to the network to access or delete information that's important for software development.
4. Laptops and handheld computers pose special physical security risks. Anyone can easily steal the entire computer and data stored on its memories (disk) as well as network logon passwords that may be saved
5. Now-a-days printers store document contents in their own on-board memories. A hacker could steal the printer to accesses the memory to make copies of recently printed documents.
6. Information on backup tapes, disks, or discs can be stolen and used by someone outside the company.

Physical security describes security measures that are designed to deny unauthorized access to facilities, equipment and resources, and to protect personnel and property from damage or harm (such as espionage, theft, or terrorist attacks). Some security measures are:

1. IT equipment and information that require protection should be placed in secure physical
2. Protection against malicious code
3. No access control during ordinary office hours.
4. Internal and sensitive information should not be printed out.
5. All printouts should be protected with "Follow me" function.

2) Loss of Authentication

Authentication is the act of determining the identity of a user and host involved in the system or software project. The goal of authentication is to first verify that the user, either a person or system, which is attempting to interact with system is allowed to do so. The second goal of authentication is to gather information regarding the way that the user is accessing system.

The ultimate responsibility of security system is to provide security to the assets so that unauthorised user cannot access information without authentication. Software developers follow the general lists of security features such as password protection, biometric details of user, firewalls, virus detection tools, etc. These implementation mechanisms are intended to satisfy authenticated access

3) Loss of Access Control

Authorization is the act of determining the level of access for authorized user. Malicious users always try to break the systems and in response, software vendors started providing security as a necessary feature for their products and network systems. Some security measures are given below:

1. Secure areas should have suitable access control to ensure that only authorized personnel have access.
2. Authorizations should only be granted on a "need to know" basis, and regulated according to role.
3. The IT department is responsible for ensuring that network access is granted in accordance with access policy.
4. Access to information systems should be authorized by immediate superiors in accordance with the system owner directives. This includes access rights, including accompanying privileges.

4) Loss of Audit

Audit is a systematic, independent and documented process to obtain audit evidences and their examination with impartiality to establish the degree in which the audit criteria are met. The experts having specific qualifications conduct the audit process independently. The audit process is closed when the activities included in audit plan are accomplished and the audit report was approved and distributed. The audit program is a document used to organize audit processes. The risk associated with audit could be in records of the audit program due to improper audit process i.e., Audit plans; Audit reports; Noncompliance reports; Reports for corrective and preventive actions; Follow-up activities reports; Results of audit program analysis.

5) Loss of Confidentiality

The property that information is not made available or disclosed to unauthorized individuals, entities, processes. There are several possible types of threat to information, some of them may be: Software threat may be defined as unauthorized disclosure, unauthorized alteration, unauthorized unavailability which could be prevented in a successful manner. Prevention of unauthorised disclosure and unauthorized alteration of information is called confidentiality and integrity. Storage and transfer of sensitive information should be encrypted or otherwise protected

B. Second phase of Framework

1) Risk Management

Risk Management identifies the possible security measures, and decides which to choose, based on two main principles: first is to ensure complete coverage and another is the expenditure on security measures, and their benefits. These

principles should be commensurate with the risks. [6] Risk management is the set of activities used to manage risks. Risk management usually consists of some major processes: Risk management planning, risk identification, risk analysis, risk planning/mitigation, and finally risk monitoring and controlling [8]. Risk management minimize, monitor, and control the probability and/or impact of unfortunate events [5].

Security is very necessary aspects that can be most considerable factor in early stage of software development Security risk analysis is concerned with identifying and evaluating risks to a system, and then security risk management allows make decisions on appropriate security measures.[6] Assessing risks means determining the effects of potential risks. Risk assessment combines the results of vulnerability analysis with the impact valuation of threats to assets, and reaches an overall conclusion about the level of risk to an asset. Risk assessments involves in identifying hazards, deciding who might be harmed and how, evaluating risks and deciding on precautions in continuation. Also, it records our findings and implementations, and regular updates and reviews [5]

2) Risk Identification

Risk is most often defined by three components that are threat, vulnerability and impact on software project. Risk identification is a process to determine threat, vulnerability and risk impact on software project. The proper identification of risk and appropriate selection of countermeasures reduces the probability to develop unsecure software. Risk identification involves gathering information about the project and determines the potential risk. It identifies known and predictable risk. Some typical techniques like assumption analysis and checklist. Normally organization uses the risk assessment checklist as a highest level of the documents for assessment. The Checklist prioritize and categorize the identified risks The risk could be related to system complexity, new technology or methodology involved that cause problems like poor design and code quality.[14] List of possible risk with which effect successful outcome of the project if the out of risk identification.

3) Software Risk Analysis:

Risk analysis is the process to identify, assess, and reduce risk to an acceptable level. It defines and control threats and vulnerabilities. Software Risk analysis evaluates criticality of the system in software design phase to introduce the significant counter measures.[14] The main objective of risk analysis is to verify and correct attributes after properly understanding the risk. Successful risk analysis include important element like problem definition, problem formulation, data collection. Some typical techniques like performance models, cost models and checklist.[8] Risk prioritization is process to set the identified and analysed risk item in ranked order form. It includes some typical techniques like risk exposure analysis and risk reduction leverage (particularly involve cost-benefit analysis) etc. [8]

4) Software Risk Response Planning

Software Risk response planning phase is very significant to develop response to appropriate identified risk which are achievable and affordable. There are several possible responses or strategies are used in risk response planning such as avoid, transfer, mitigate and accept etc.

5) Risk Mitigation

Risk mitigation planning is the process of controlling actions which are identified and selects suitable ones to reduce threats according to project objectives. It includes risk monitoring and enhances identified risk tracking, evaluating risk process effectiveness throughout the project and implements risk mitigation action [15].

C. *Third Phase of framework*

1) Documentation

Documentation is very relevant for overall software development. A formal document is prepared after risk reduction approval, which contains a complete description of the external and internal behaviour of the software system. Documentation of project minimizes the time and effort required by developers to achieve desired goals and also minimizes the development cost. It defines how an application will interact with system hardware, other programs and users in a wide variety of real-world situations. Parameters such as operating speed, response time, availability, portability, maintainability, footprint, security and speed of recovery from adverse events are evaluated in documentation.[14]

III. CASE STUDY

The proposed framework has been illustrated with a case study to reduce the PRR and implement the security factors. This case study is done on unique identification project (UID). Framework is applied to UID project. Here project related risks are considered. The PRR are examined for high or low levels of risk. PRR with high risk are assessed to identify and analyse risk factors. The risk factors of PAAAC (physical security, authentication, access control, audit, confidentiality) are identified, given in Table I. The identified risk is reduced through the risk mitigation method. The risk mitigation methods are used in the UID project, i.e., Aadhar card.

TABLE I. UID case study based on PAAAC Framework

Loss of:	Risk	Results after mitigation
Physical security	• Card damage • Data lost • Improper demographic details • • Data could be misused or theft	• If the card is damaged or theft then online ID platform is available • Proper demographic details.
Authentication	• Anyone can change identity • No unique identity • Difficult to identify fake document and copies • Can not verify that the person defined in the identity token is indeed the same person defined in the identity	• It provides uniqueness • No one can change identity • Only beneficiary can utilize the services. • Prevent duplicity through biometrics details(finger prints, iris)
Access Control	• Unauthorised access • Unrestricted system use	• Authorised access • Restricted system use • No one can access the data due to biometric details.
Audit	• Difficult to identify fake document and copies • Improper detection of data entry error. • Manual data entry error such as: if two or more people are namesake it could create problems; due to illiteracy, some people are not able to recognise any mistake, if there in the identity card.	• Unique database. • Uniqueness and Existence ensures no fakes or duplicates • To prevent duplicity it Clean up existing databases through Uniqueness
Confidentiality	• Due to manual data entry it could be misused. • Duplicity • Forgery of identity cards	• Difficult to identify fake document and copies • Improper detection of data entry error. • Manual data entry error such as: if two or more people are namesake it could create problems; due to illiteracy, some people are not able to recognise any mistake, if there in the UID

Aadhar Card is basically a proof of the unique identification of every individual. It provides every individual with a unique Identification Number (UID). It is meant for individuals of any age including children, and its main purpose is to establish identities. The Aadhar project has grave civil liberty implications. It will enable the government to profile citizens and track their movements and transactions. One more advantage of Aadhar card is that after entering a individual's name or Aadhar no. all of his/her details can be accessed, for example colour of his/her car traffic fines to be paid and last time he/she paid for a bill etc.

After the use of risk mitigation methods some risks are left. These are:

1. No fail-safe against misuse
2. Ambiguity in biometric data

One drawback of Aadhar is that people with low- quality fingerprints, such as the construction workers or people having cataract/ comeal problems, face problems with fingerprints and iris scans. Another major limitation is the fact that data theft has been a very serious problem in today's technological world. This raises the concern for data security of Aadhar

cards. Data theft and transfer to intelligence agencies or corporations have potentially horrendous consequences. Now, we have to iterate the risk removal process again for approval of risk reduction.

IV.FUTURE SCOPE

As a future work, a researcher can improve the proposed framework to manage all external and internal PRR risks that may affect the software project. Another extension is to focus on more detailed risk management for PRR. A particular risk of PRR can be extended and incorporated for the development of secure software. And finally, the work can be extended by exploring and utilizing other more effective techniques to mitigate the PRR.

V. CONCLUSION

It is found that there are insufficient framework are available which can mitigate PRR insufficient manner. However, some framework provides good approach to reduce the risk from software system but they are expensive and time consuming in nature. A framework is proposed to analyze and mitigate PRR and implement secure software. The ultimate goal of proposed framework is to secure assets from PRR, which can harm the assets. It improves the software quality and delivers secure software project through the different phases of framework accompanied with the iterative risk management steps. The proposed framework will be helpful for analysts and security engineers to incorporate security features in software development.

REFERENCES

[1] H. Hoodat, H. Rashidi. "Classification and analysis of risks in software engineering", World academy of science, Engineering and Technology, vol. 1 No.5, 2009.

[2] J. Kontio, "The risk method for software risk management", Institute for Advance Computer Studies and Department of Computer science, University of Maryland, 1999.

[3] H. Ronald, P. Haimes and Y. Yacov, "Software risk management", *University of Virginia: Software engineering institute, Centre for risk management of engineering*, 1996.

[4] Dhirendra Pandey, Ugrasen Suman & A. K. Ramani, "Security Requirement Engineering Issues In Risk Management", *International Journal Of Computer Applications, Foundation Of Computer Science*, USA, ISBN: 978-93-80747-89-4, Vol. 17, No. 5, Pp.11-14, 2011.

[5] Dhirendra Pandey, "International Journal of Computational Intelligence And Information Security", *IJCIIS*, Australia, Vol. 1 No. 8, Issn: 1837-7823.

[6] Dhirendra Pandey, Ugrasen Suman and A. K. Ramani, "Security Requirement Engineering Framework for Developing Secure Software*", International Journal of Computational Intelligence and Information Security, IJCIIS* Australia, Vol. 1 No. 8, Issn: 1837-7823, Pp.55-65, 2010.

[7] A Framework for Modelling Software Requirements IIJCSI (International Journal Of Computer Science Issues), Vol. 8, Issue 3, No. 1, May 2011 Issn- 1694-0814.

[8] Richard Failey, "Risk management for Software project*", IEEE Computer Society*, vol. 11, pp.57-66, May 1994.

[9] Gary Mcgraw, "Risk analysis in software design", *IEEE Computer Society*, pp.79-84, August 2004.

[10] Deniz Kasap, Murat Kaymak, "Risk Identification Step of the Project risk Management" PICMET Portland USA, pp.2116-2120, August 2007.

[11] Mumtaz Ahmad Khan, Shadab Khan, Mohd Sadiq, "Systematic review of software risk assessment and Estimation Models", *IJEAT*, vol-1, Issue1, April 2012.

[12] Roger S Pressman," Software Engineering- A Practitioner's Approach", *McGraw-Hill Series in Computer Science*,2006

[13] Ahdieh Sadat Khatavakhtan, Siew Hock Ow, "An innovative model for optimizing software risk mitigation plan: A case study", *IEEE Computer Society*, pp.220-223, May 2012.

[14] Dhirendra Pandey, A. K. Ramani, U. Suman, "An Effective Requirement Engineering Process Model for Software Development and Requirements Management", *International Conference on Advances in Recent Technologies in Communication and Computing, pp.287-291*,2010.

