Validation of SIS Framework using ASP/JSP Based Information System

D. NagaMalleswari, K.Subrahmanyam

Abstract: Software Products are developed so as to fulfill the gathering of conditions and needs of a bunch of business individuals. The software quality is much concerned because the failure or a software error may cause in terms of finance and organisation reputation. So identifying and mitigating the risks in software is a continual process. Risk Management is important for an information system. Risk management helps in mitigating risks and their effect on the information system. For doing so the SIS framework will assist. In this paper, we are going to evaluate the validation of the SIS framework. We will be assessing the framework on how it recognises and treats the risks in the information system. It is a quantitative and qualitative approach and is used to manage risks in information system so that the system can operate properly and securely.

Keywords: Risk Management, Performance evaluation, Validation, SIS framework

1. INTRODUCTION

Risk is a probable issue or loss that may or may not occur in future which may have adverse impact on the system. Risk can be perceived as uncertainty having its effect on the system. So it is important to understand risks and reduce them. For this risk management is to be done. The prime aim of risk management is identifying and controlling all possible risks before they occur in the system. Risk management is a process of identifying, assessing risks and utilization of measures to limit, screen and control likelihood or effect of the uncertainties. It means that we need to identify risks in the system, assess them for their likelihood, consequences or effect on the system and tolerability and ways to reduce them. Conducting systematic risk management can help in mitigating risk along with its impact on the system and not hinder the performance of the system.

In order to have an effective validation we are proposing a method in this paper which includes of majorly three parts they were SCARE, Information Acquirement, and SWOT analysis. By using this three performance measures we can assure that the risks can be identified and assessed easily and effectively.

2. LITERATURE REVIEW

Risk Management can be defined as the process of risk assessment and mitigation. Better software helps an organization or institution to grow better, where faulty or error software may lead an organization go worse. The software failures are causes by the risks. It is observed that the risks have been arising in software at five different areas in the process of development and the maintenance of a software product [1]. They are Participants, Environment, Technology, Infrastructure, and Information.

Assessing and analysing of risks are the keys ways in which we eradicate risk and create the project successfully.

Assessment of risk can be done in many ways and plenty of additional strategies were projected. A number of them were assessed manually which is not a best practice. We are mainly focused on the assessment of risk based on the source code evaluation. We found few models assessed based on the source code through gathering information and reviews conducted with the stakeholders. Few proposed models of risk are divided into dynamic and static risk assessment models [2]. After a deep study of different methods we finally came to an understanding that for an effective risk assessment can be done with the help of the SCARE Information Acquirement and the SWOT analysis.

3. METHODOLOGY

There are many traditional methods where the risks are calculated manually by conducting a series of interviews and review meetings among the group of so called officials of the organisation and the stakeholders. This method of risk assessment is not a best practice as it does not takes the complete software system into consideration i.e, the source code and various methods used for obtaining the different major functionalities in a software product.

Now our proposed method over- comes the problems mentioned above and this method considers the source code analysis and risk evaluation (SCARE) to analyse and assess the complete source code of a software system, and the information acquirement to consider the view of the stakeholders of a software system and finally the SWOT analysis which is used to take the inputs from the experts working on the software system.
From the above fig it is clear that any process related to the risk come under the risk management process. The First step in this process is Risk Identification. This risk identification in our method is done by using the following three approaches:

Source Code Analysis Risk Evaluation (SCARE)

In this risk is evaluated by examining the source code of the system. Source code being one of the major part of the system, it contributes in identifying the risk largely. We use cyclomatic complexity to calculate the complexity of the program of the system which helps to assess the risks. Based on this complexity, we can understand the seriousness of the risks in the information system. Then it can also help in doing any improvements to the system. We consider five factors namely, people, infrastructure, technology, environment and information while doing SCARE. In this framework to recognize the risks we consider 60% from SCARE itself.

Information Acquirement

For acquiring the information we prepare questions for a website in general considering all the five factors that are people, infrastructure, environment, technology and information. Then we do a survey and collect responses from professionals. Then we can evaluate risk by applying confusion matrix on it.

Confusion matrix is one of the methods which is used to measure performance of classification models. It is also known as error matrix. Using confusion matrix we can calculate accuracy and error rate which will help in identifying the risk in the system. We consider 30% of information acquirement in the SIS framework

SWOT Analysis

The SWOT Analysis is basically done with the help of the expert judgement system. It involves asking questions to the people who are experts in the industry. Then their feedback is taken which helps in identifying the risks in the system. Here also the five factors are considered. 10% of the SWOT analysis is considered in the SIS framework.

Using the Cyclomatic complexity as a primary issue for associate degree application or a system helps the organization to spot the foremost risk parameters and helps to develop for the advance or the adjustment approaches to scale back the threats or known risks, repair time, productive problems, technical problems within the software. Based on the obtained cyclomatic complexity we are going to assess the software risk present in any software product as mentioned by McCabe labs through their research study.

<table>
<thead>
<tr>
<th>Complexity Number</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-10</td>
<td>Structured and well written code HighTestability Minimal Risk</td>
</tr>
<tr>
<td>10-20</td>
<td>ComplexCode MediumTestability Moderate Risk</td>
</tr>
<tr>
<td>20-40</td>
<td>VerycomplexCode LowTestability High Risk</td>
</tr>
<tr>
<td>&gt;40</td>
<td>Notatalltestable Very high risk</td>
</tr>
</tbody>
</table>

4. RESULTS

R&D Progress reviews application is used to identify the risks where cyclomatic complexity is calculated and using the approach proposed by McCabe software labs

![Fig: R&D Progression Reviews Application](image-url)
Fig: 2 Risk Calculation for participants

Fig: 3 Risk Calculation for Environment
Fig4: Risk Calculation for Infrastructure

Table: Risk for the R&D Progress Review Application

<table>
<thead>
<tr>
<th>Factors</th>
<th>Cyclomatic Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participants</td>
<td>18</td>
</tr>
<tr>
<td>Environment</td>
<td>28</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>20</td>
</tr>
<tr>
<td>Technology</td>
<td>14</td>
</tr>
<tr>
<td>Information</td>
<td>17</td>
</tr>
</tbody>
</table>

Hence it is observed that for the factors like Participants, Technology, and Information the risk is moderate and medium testability and for the other factors like Infrastructure and Environment the risk is high and low testability.

5. REFERENCES

1. Risks Armen Keshishian1, Hasan Rashidi21Computer science Dept, Qazvin Azad UniversityIran, Tehran 2Hasan Rashidi, Qazvin Azad UniversityIran, Tehran
3. Maruf Pasha1, Ghazia Qaiser1, Urooj Pasha2" A Critical Analysis of Software Risk ManagementTechniques in Large Scale Systems” 2169-3536 (c) 2018 IEEE.
8. W. Eric Wong, Yu Qi, and Kendra Cooper Department of Com-puter Science University of Texas at Dallas Richardson, TX 75083 {ewong, yxq014100, kcooper}@utdallas.edu
11. Mir ShahriarEmami; NorafidaBintiIthnin ; Othman Ibrahim “Software process engineering: Strengths, weaknesses, opportunities and threats” INC2010: 6th International Conference on Networked Computing