ISSN No. 0976-5697

Volume 1, No. 3, Sept-Oct 2010

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Risk Assessment Framework (RAF)

S. K. Pandey * & Mustafa K.
Department of Computer Science
Jamia Millia Islamia (Central University), New Delhi-110 025, India
E Mail: santo.panday@yahoo.co.in, kmfarooki@yahoo.com

Abstract: Today's business is very much dependent on the information systems. Computer networks have transferred our life into a fast and comfortable one but at the same time, it has posed various threats to the existing information system due to open accessibility. Any information asset, when connected to the outside world, is vulnerable to attacks. The attacks are mainly caused by threats that have the potential to exploit vulnerabilities. Any type of damage to these assets causes risk and it is one of the most important factors to the organization. The risk of malicious attacks to the software security has considerably gone up and to prevent such risk is very necessary. The maxim *'sooner is better'* has become the order of the day. Hence, this study was undertaken in view of the significance of risk assessment in the requirements phase of SDLC. In the absence of any roadmap/process/framework, in this paper, we hereby propose Risk Assessment Framework (RAF) for assessing the risk in the requirements phase itself along with validation results. This framework has three major components: nine security policies checklists, weightage for the attributes of each policy and quantified risk estimation. Such a framework may prove to be relevant at mitigation of security vulnerabilities, right from the beginning i.e. requirements phase and lead to considerable reduction of cost in terms of software security assurance.

Keywords: Risk Assessment, Risk Assessment Framework, Information Security, Quantitative Assessment of Risk.

I. INTRODUCTION

The modern technology is at the helm of development and progress. The progress has been achieved but this has some limitations too. These limitations are posing big threats and challenges and these are required to be addressed by software experts. Some of the software are being developed and put into test to thwart and minimize the risk. It is noteworthy to mention that the assessment tests are to be nominated and in the application of security measures. Time should be managed in order to maintain accuracy and speed up the security process.

Scorpion's efforts are being attempted to develop secure software but these are not sufficient and satisfactory, as it may delay security assessments. Such 'delays' may count heavily towards security and quality assurance measures (Pandey, S.K. et al., 2007, December). It is observed that the development in respect of early and accurate security estimation needs to be undertaken for holistic developments. It is imperative to have a potentially effective approach for an early, on time and accurate assessment of risk during software development life cycle.

Traditionally, risk can be defined as the potential harm caused if a particular threat exploits a particular vulnerability to cause damage to an asset, and risk analysis is defined as the process of identifying security risks and determining their magnitude and impact on an organization (Mazumdar, Chandan et al., 2007) (Hirsch, Corey & Ezingeard, Jean- Noel, 2008). NIST Guide for Security Certification and Accreditation (Stoneburner, Gary et al., 2002, July) elaborates the definition to explore the entire process. Risk assessment comprises of three major areas, as: (i) Identification of threats to and vulnerabilities in the system; (ii) Potential impact or magnitude of harm that a loss of CIA (Confidentiality, Integrity or Availability) would have on enterprise operations or enterprise assets, should an identified vulnerability be exploited by a threat; and (iii) The identification and analysis of security controls for the information system (Abdullah, Tahir et al., 2010).

At present, Risk assessment is an instrumental technique for managing Information Systems Security (Alen Julia et al., 2008). Various information security risk assessment methods are available that can be adapted and executed by the organizations, and each has different approaches to assess and monitor the information security risks (Ashbaugh, Douglas A., 2008). A comparative study of the major existing frameworks, COBRA, CORAS, CRAMM, OCTAVE, SOMAP, and NIST Guide, along with strengths and weaknesses of each one has already been accomplished (Mustafa, K. & Pandey, S. K., 2010, January). To surpass these weaknesses and realizing the need of a risk assessment methodology particularly for requirements phase of SDLC, ahe new framework RAF is proposed. This work unfolds and provides an integrated method to determine the risk in a quantitative manner that may be presented at the requirements phase itself.

The rest of the paper is organized as follows: Section II presents a brief discussion on the RAF Process, whereas in Section III, Implementation Mechanism is discussed. In Section IV, an Inplementation Example is discussed followed by Tryout Results on the SRS of a live project given in Section V. Section VI presents Conclusion and Future Research Directions in the area.

II. RAF PROCESS

A prescriptive Risk Assessment Framework (RAF) is hereby proposed for the risk assessment in the requirements phase of SDLC. By adopting RAF, a requirement engineer can assess the risk aspects of SRS in a right perspective. RAF is a cyclic process in which a number of steps/stages are involved to reach the ultimate objective. The architecture of RAF is given in the Figure 1.

RAF is a security risk assessment framework for requirement phase. By going minutely, its various stages, requirement engineers would be able to assess the risk aspects of the requirements. RAF will be operated on SRS, prepared by requirement engineers. The impetus acknowledged is on security policies and its checklists. In each security policy, various attributes are identified based on the checkpoints and then the respective weightages of each one is also assigned through an estimation using expert surveys. A mathematical formula is proposed for the calculation of the risk. Then the tolerance level of the risk is also assessed and accordingly, so

that the suitable countermeasures/ mitigation techniques can be applied in a smooth manner. If risk is acceptable according to the time, type of project as well as resources available, then SRS could be delivered for design phase.

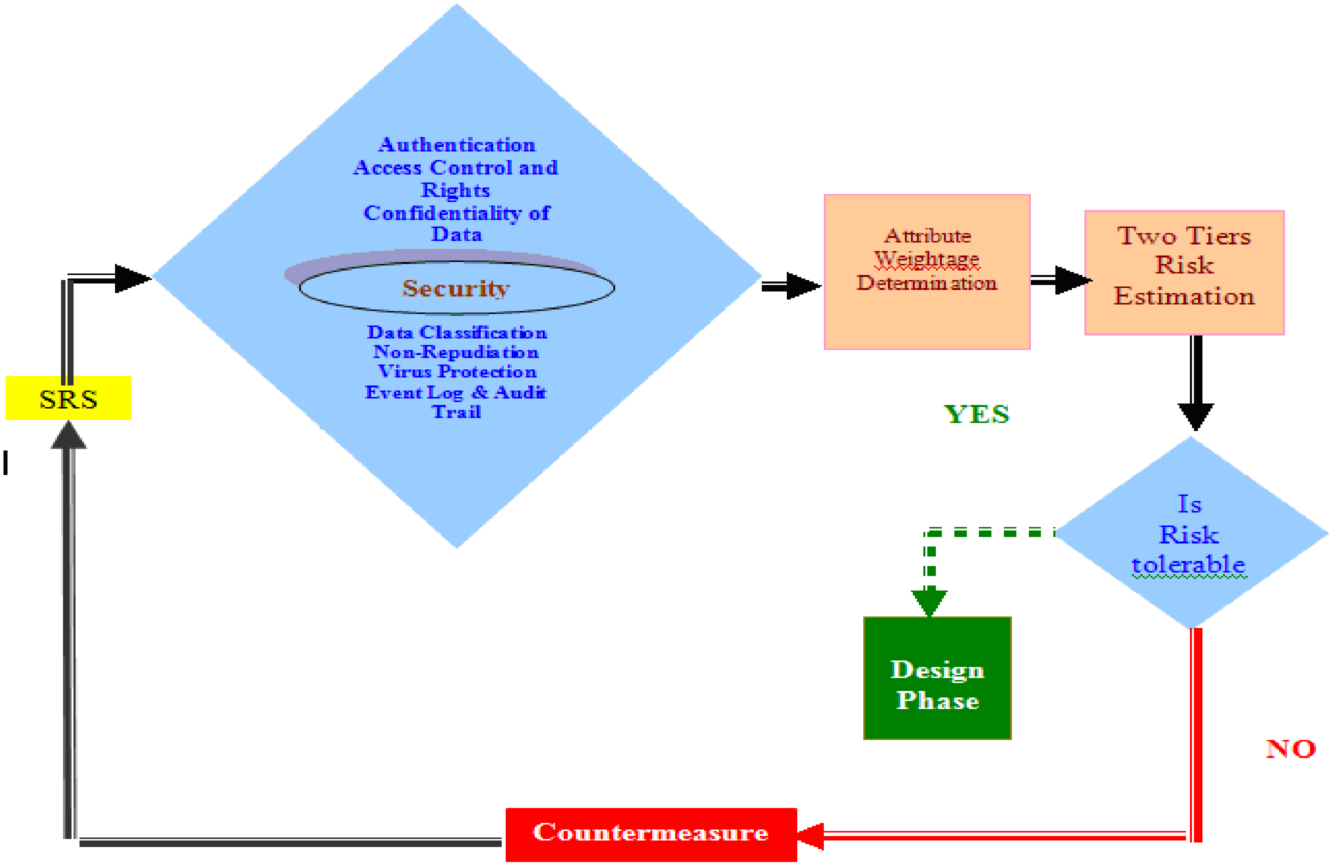

Figure 1. Architecture of the RAF

A. *Security Policies*

In general terms, security policy typically describes principles or rules to guide decisions and achieve rational outcomes for assuring information Systems for organization or other entity. These are of prime importance for risk management, fraud prevention, and information teams. The security policy addresses constraints on functions and flow among them, constraints on access by external systems and adversaries including programs and access to data by people. Sound security policy architecture protects organization from attacks as well as accidental internal leakage of information, and data mishandling, whereas a poorly documented or ambiguous policies may result into a production delay and confuse the security team members which results in higher cost and effort. These nine security policies are shown in the first part of this figure. For this purpose, a checklist is proposed for each of the security policy. Due to page limitations, we are not giving the complete checklists in this paper. Some of these checklists have already been published (Mustafa, K. et al., 2008) (Mustafa, K. et al., 2009) (Mustafa, K. & Pandey, S. K., 2010, July) (Mustafa, K. & Pandey, S. K., 2010, Aug). S. No. of checkpoints/attributes of the policies does not refer any priority of the attribute, it is used for only convenience of the presentation.

B. *Determination of the weightage of the attributes*

After the designing of these checklists, it was felt by a team of experts that each checklist contains various attributes corresponding to each checkpoint and hence their weightage for that security policy may not be the same rather it will be definitely different. Thereby, a process of estimating component weightages (e.g. quantified impact) initiated through well structured expert survey by area experts/practitioners. The feedback was collected on the following issues:

- Checklists' relevance to the purpose,
- Analysis of the checklists' quality which include following heads:
  - importance of the attribute
  - Potential utility for evaluation practice
  - Completeness/coverage of attributes
  - Relevance of all the attributes
- In the rightmost column of each checklist, to assign a *weightage between 1 to 5 (1 is minimum and 5 is maximum)* to each attribute for the implementation of the each security policy.

These checklists along with the review form were sent to the thirty experts from the varied fields' viz. academia, industry, scientific organizations, educational institutions, research bodies, government organizations. After a comprehensive exercise, we were able to have duly filled feedback forms from the twenty experts only. After collecting these forms, feedback was compiled in two ways. At first level, based on the comments cited in the review forms, we made some revisions in the checklists/attributes and then again a fresh ranking was taken. At the second level, we designed a format in an excel sheet, in which all the data from the experts' comments were filled. Since, we received the feedback from twenty experts only; an average rank value of each attribute was calculated. Based on the average value of each attribute, we finalized the weightage of the attributes of each security policy which are tabled in the following sections along with some description of each policy:

a)Authentication Policy : In order to prevent software from various business and environmental hazards, systems and procedures are being developed and implemented for authentication of users so that only authorized users given access to the application. Strong authentication process should be adopted for all critical applications & databases. For the Authentication Policy, the attributes' weightage is given in Table 2.1:

Table 2.1: Attributes' Weightage of Authentication Policy

S. No.	**Attribute**	**Attribute's Weightage**
1.	*Access Control*	4.75
2.	*Authorized Application Access*	4.4
3.	*Confidentiality Agreement*	3.95
4.	*OS Level Access Control*	3.9
5.	*Database Access Control*	4.6
6.	*Password Standardization*	4.35
7.	*Confidentiality of Passwords*	4.4
8.	*Multilevel Authentication*	4.1
9.	*Password Expiry*	3.8
10.	*Password Changing Procedure*	3.95
11.	*Login Interface Capability*	4.15
12.	*Password Resetting Verification*	3.95
13.	*Password Encryption*	4.4
14.	*Physical Security of Password*	4
15.	*Accounts locked out*	3.95
16.	*Changing default Password*	3.8
17.	*Password Policy*	4.3
18.	*Audit Trail*	4.35
19.	*Session Cleanup*	4.15
20.	*Access Attempt*	4.15
21.	*OS Level Authentication*	3.85

b) Access Control and Rights Policy: To safeguard software systems, procedures are being developed and implemented for protecting them from unauthorized modification, disclosure or destruction. It is done to ensure that information remains accurate, confidential, and can be made available at the time of requirement (Computer Technology Documentation Project, 2009). For the Access Control & Rights Policy, the attributes' weightage is in Table 2.2:

Table 2.2: Attributes' Weightage of Access Control and Rights Policy

S. No	Attribute	Attribute's Weightage
1.	*Business Access Control*	4.5
2.	*System Related Access Control*	4.4
3.	*Trade-off*	3.95
4.	*User level Authentication*	4.5
5.	*Access Control*	4.75
6.	*Master Record Maintenance Mechanism*	4.75
7.	*Formal Authorization*	4.55
8.	*Unique IDs*	4.15
9.	*Permission*	3.8
10.	*Disabling*	4.35
11.	*Validity*	4.65
12.	*Changing Default Passwords*	4.35
13.	*ID Expiration*	4.2
14.	*Audit trails*	4.4
15.	*Session Cleanup*	4.1
16.	*Audit Trail Review*	4.1
17.	*Encryption*	4.6
18.	*Read Only Facility*	4.25
19.	*Write/update Facility*	4.2
20.	*Account locked out*	4.05
21.	*Automatically get locked*	4.5
22.	*Correct Timing*	4.25
23.	*Periodicity*	4.3

c) 'Confidentiality of Data' Policy: Software should provide maximum protection to classified, sensitive and confidential information identified by the company for efficiently utilizing data encryption. Need and the extent of utilization of data encryption methods shall be justified by clear and transparent business objectives, nature of technology, information classification and the resultant risk to the information resources. For the 'Confidentiality of Data' Policy, the attributes' weightage is in Table 2.3:

Table 2.3: Attributes' Weightage of 'Confidentiality of Data' Policy

S. No.	Attribute	Attribute's Weightage
1.	*Consistency Check*	4.53
2.	*Possibility check*	4.35
3.	*Information/ Data Access Control*	4.59
4.	*Information Request Handling Mechanism*	4.41
5.	*Trade-off*	4.24
6.	*Information/Data Encryption*	4.88
7.	*Log File Maintenance*	4.76
8.	*Information/Data Ownership*	4.76
9.	*Periodicity v/s Validity*	4.29
10.	*Validity*	4.47
11.	*Permission*	4.35
12.	*Dissemination*	4.35
13.	*Identification*	3.94
14.	*Garb-aging*	3.88

d) Encryption Policy: The purpose of this policy is to set a guideline for usage of encryption methods and management of the encryption software for maintaining integrity and confidentiality of information in storage and during transit. The organizations should provide maximum protection to classified, sensitive and confidential information following by efficiently utilizing data encryption. The need and the extent of utilization of data encryption methods is justified by well set business objectives, nature of technology, information classification and the resultant risk to the information resources (National Thermal Power Corporation Ltd., 2006, July). For the Encryption Policy, the attributes' weightage is in Table 2.4:

Table 2.4: Attributes' Weightage of Encryption Policy

S. No.	Attribute	Attribute's Weightage
1.	*Third Party Transmission Checkup*	4.45
2.	*Encryption of Confidential Information*	4.85
3.	*Separate Encryption Keys*	4.80
4.	*Portable Disk Information Encryption*	4.60
5.	*Encryption Information in Storage Media*	4.70
6.	*Encrypted Password Backup*	4.65
7.	*Preventive Hard Disk Checkup*	3.95
8.	*Standard Encryption Algorithms*	4.70
9.	*Authorized Personnel Accessibility*	4.60
10.	*Secured Encryption Facility*	4.55
11.	*Periodic review of Algorithms and Standards*	4.80
12.	*Uncompromised Encryption Keys*	4.65
13.	*Single Purpose Key*	4.25
14.	*Periodic Change of Encryption Keys*	4.40
15.	*Aligned/ Synchronized Data Encryption and Decryption Checking*	3.95
16.	*Encryption Key Access Control*	4.5
17.	*Encryption of Encrypted Keys*	4.95
18.	*Master Keys Transmission*	4.6
19.	*Storage of Master Key*	4.45
20.	*Material Elimination*	4.4
21.	*Encrypted/ decrypted Enabled Functions*	4.25
22.	*Key Inclusion in Escrow Management*	4.1
23.	*Secure Encrypted Channel*	4.8

e) Data Classification Policy: Data classification policy is designed to ensure the integrity and confidentiality of information (National Thermal Power Corporation Ltd., 2006). The level of security to be afforded to the data/information of the company depends directly on the classification level of the data. The data/information of the organizations largely tours upon the classification level of data. However, it is expected from all the employees of the company to remain familiar with the data classification scheme and use it on a regular basis. For the Data Classification Policy, the attributes' weightage is in Table 2.5:

Table 2.5: Attributes' Weightage of Data Classification Policy

S. No.	Attribute	Attribute's Weightage
1.	*Procedure for Data Classification*	4.35
2.	*Authorization*	4.85
3.	*Data Classification Policy*	4.85
4.	*Sustained Protection*	4.40

5.	*Implementation of Classification Rules*	4.65
6.	*Data Classification Responsibilities*	4.55
7.	*User Compliance*	4.65
8.	*Disclosure of Data*	4.30
9.	*Migration of Unstructured Data*	4.35
10.	*Automatic Classification*	4.45
11.	*Usability of Data Classification Rules*	4.55
12.	*Granular Data Sorting*	4.35
13.	*Data Transfer*	4.20

f) Non-Repudiation Policy: Non-Repudiation denotes 'Not denying or reneging'. Digital signatures and certificates offer non-repudiation as they guarantee the authenticity of a document or message (Mccullgh, Adrian & Caelli, William, 2000). For the Non-Repudiation Policy, the attributes' weightage is in Table 2.6:

Table 2.6: Attributes' Weightage of Non-Repudiation Policy

S. No.	Attribute	Attribute's Weightage
1.	*Authentication by Digital Signature*	4.50
2.	*Compliance with IT (Amended) Act, 2008*	4.70
3.	*Information Accessibility and Usability*	4.40
4.	*Accuracy of Information*	4.65
5.	*Metadata of Document*	4.60
6.	*Uniqueness of Digital Signature*	4.25
7.	*Capability of Digital Signature Integrity*	4.45
8.	*Private Key*	4.45
9.	*Certifying Authority*	4.40

g) Virus Protection Policy: A computer virus is commonly known as an unauthorized and malicious program, which replicates itself and spreads onto various data storage media such as floppy diskette, magnetic disk, tapes and across the network. The organizations should protect its IT resources from all possible computer virus and related threats by deploying the procedures and best practices. For the Virus Protection Policy, the attributes' weightage is in Table 2.7:

Table 2.7: Attributes' Weightage of Virus Protection Policy

S. No.	Attribute	Attribute's Weightage
1.	*User Training*	4.40
2.	*Antivirus Installation*	4.90
3.	*Antivirus Maintenance and Up-gradation*	4.90
4.	*Recovery Assistance*	4.50
5.	*Critical Areas Analysis*	4.55
6.	*Auto-scans Configuration*	4.55
7.	*Updation of Antivirus*	4.60
8.	*Caution for Attachment*	4.25

9.	*Individual Regular Backup*	4.30
10.	*Automatic Downloading of Antivirus Definitions*	4.90
11.	*Antivirus Installation in Totality*	4.85
12.	*VBS Scripts Gateway Checking*	3.95
13.	*.EXE Files Gateway Checking*	3.90
14.	*Disabled Antivirus Protection*	4.15
15.	*Scheduled Scanning*	4.3
16.	*Forced Media Scanning*	3.65
17.	*Periodic Review of Antivirus Logs*	3.9

h) Event Log and Audit Trail Policy: In order to safeguard information and computing resources from various business and environmental threats, systems and procedures must be developed and implemented to monitor the activities related to the use of the Information System resources. It is very vital to ensure that the information on these systems is not revealed to unauthorized individuals, and that the integrity of the data is restored. Company should therefore have a policy for maintaining the event logs and audit trails, preventing and detecting any unwanted tampering and use of its IT resources. For the Event Log and Audit Trail Policy, the attributes' weightage is in Table 2.8:

Table 2.8: Attributes' Weightage of Event Log and Audit Trail Policy

S. No.	Attribute	Attribute's Weightage
1.	*Employees Accountability*	4.45
2.	*Security Breaches Reporting*	4.65
3.	*IT Resource Sabotage*	3.85
4.	*Compliance Monitoring*	4.55
5.	*Record Keeping of Audit Trails*	4.60
6.	*Systems Monitoring*	4.45
7.	*Security Log Reports*	4.70
8.	*Firewall Activation*	4.55
9.	*Internet Connection Periodic Review*	3.90
10.	*Intrusion Detection Systems*	4.65
11.	*System Monitoring Tools*	4.15
12.	*Critical Data*	3.60
13.	*Security Environment Periodic Review*	4.25
14.	*IT Users Practice Monitoring*	4.45

i) Backup and Recovery Policy: Backup of all business data, related application systems and operating systems software should be taken on a periodical basis, as to protect information and computing resources from various business and environmental threats. This Policy applies to all the employees of company as well as to the third parties, and all information resources including corporate data, as well as the application and systems software. For the Backup and Recovery Policy, the attributes' weightage is in Table 2.9:

Table 2.9: Attributes' Weightage of Backup and Recovery Policy

S. No.	Attribute	Attribute's Weightage
1.	*Daily Backup*	4.70
2.	*Regular Examination*	4.80
3.	*Data Backup Safety*	4.75
4.	*Periodic Backup Logs*	4.60
5.	*Periodic Backup Review*	4.75
6.	*Readability of Backup Media*	4.40

C. Risk Assessment

In the absence of any framework, fully devoted to the risk assessment in the requirements phase of SDLC, RAF is proposed to fill the gap. After determining the weightage of the attributes of the security policies, we propose the two-tier risk assessment process, which can be done by using the formulas. The formulation is done by using the concept of multivariate regression, which is a suitable statistical tool that may be used in these conditions. Here, two terms have been introduced: Policy Compliance Factor (PCF) and Risk Factor (RF). PCF refers to the overall compliance/adherence to policy checkpoints. RF refers to the quantified estimation of occurrence of the risk.

For the first level risk assessment:

Policy [Attributes]

PCF = ∑ Wi Xi ⁄ n where Xi = { 1 or 0
and i = 1, 2, 3, …………n

Here, Wi is the weightage of the attribute, and Xi is the value of the compliance of the checkpoint i.e. if a checkpoint is compliance, the value will be 1, and if not, its value will be 0.

For the second level risk asse

Risk [Policy

Low Risk
Zone

RF = ∑ Wi 1 or 0
and i = 1, 2, 3, …………n

Here also, Wi is the weightage (value) of the security policy which is calculated at the level L1, and Xi is the value of its occurrence i.e. if a security policy is applicable for a project, the value will be 1, and if not, its value will be 0. But, we strongly recommend that all these policies are applicable for building secure software.

D. Risk Tolerance

High Risk
Zone

Based on the above cal its tolerance limit may be decided. We p ng limits, as given in the Fig. 2:

- **Low Risk:** SRS is at low risk if the value of the final risk value is ≥ 3.5.
- **Medium Risk:** SRS is at medium risk if the value of the risk lies between 2.5 to 3.5.
- **High Risk:** SRS is at high risk if the risk value is ≤ 2.5.

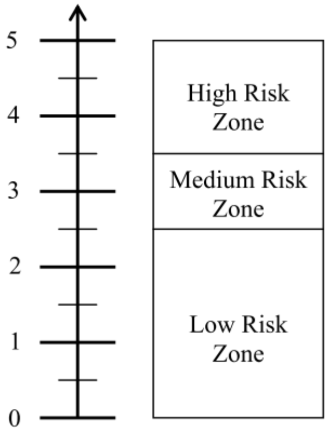

Fig. 2: Risk Zones

III. IMPLEMENTATION MECHANISM

Proposal of any framework is only useful if it is easy/handy to implement in the real life projects. We tried to make RAF user friendly from the point of implementation. Following are the guidelines/ steps for implementation of the RAF:

- SRS will be taken as input in the RAF.
- The next step as per the RAF will be structured walkthrough by checklist filtering of the SRS, in which several checklists of security policies are provided for verification of the SRS.
- If any checkpoint is not pertinent to the project, it may be identified as 'not applicable'. This will not be taken into consideration.
- For all the applicable checkpoints, requirement engineers may assess the compliance/non-compliance checkpoints.
- Accordingly, the weightage of every attribute is taken for each security policy.
- Then, the two levels of the assessment may be followed, as specified in the RAF for the calculation of the risk.
- If the risk is tolerable, then the teams should handover the final SRS to the designers. Final SRS will be the output of the requirement phase of the SDLC.
- If the risk is not tolerable, then the teams should modify the SRS and repeat the steps from beginning, iteratively.

IV. IMPLEMENTATION EXAMPLE

Considering that we are calculating the value of risk for the requirements phase for a project, we will follow the following steps:

Step 1: The first step is the assessment of the checkpoints given in the various security policies checklists. If a checkpoint is not applicable for the project, it will not be considered for the risk assessment. In rest of the points, requirement engineers will mark 'yes' or 'no'. If the answer is 'yes', its value will be 1, otherwise 0.

Step 2: Here, we will do the two levels risk assessments.

For the first level risk assessment:

Let us assume that all the checkpoints are applicable for the project.

PCF for Authentication Policy (P) = $(4.75 \times 1) + (4.4 \times 1) + (3.95 \times 1) + \ldots\ldots\ldots\ldots / 21$

PCF for Access Control and Rights Policy (Q) = $(4.5 \times 1) + (4.4 \times 1) + (3.95 \times 1) + \ldots\ldots\ldots\ldots / 23$

PCF for 'Confidentiality of Data' Policy (R) = $(4.53 \times 1) + (4.35 \times 1) + (4.59 \times 1) + \ldots\ldots\ldots\ldots / 14$

…………………………………… For all the policies

For the second level risk assessment:

We propose that all the policies are applicable for any project; hence the value of Xi will be 1.

$$RF = (P \times 1) + (Q \times 1) + (R \times 1) + \ldots\ldots\ldots\ldots / 9$$

This will be the final value of the risk.

V. TRYOUT RESULTS

The proposed framework, for the risk assessment in requirements phase has been validated by using SRS of one live project. The purpose of this SRS is to supply California State University at Northridge (CSUN) with an outline of a software product to handle the student course information process. Individuals responsible for reviewing all proposals for this software are the intended audience for this document. This may include students, faculty, administrators and any other individual who may be responsible for maintaining and upgrading the current computer system, and purchasing new systems. The software product proposed by this SRS is the Student Course Information System (SCIS).

By applying the formula given in RAF, we calculate PCF for each security policy and then RF whose value comes as follows:

$$\begin{aligned} RF &= (2.3 \times 1) + (2.10 \times 1) + (1.29 \times 1) + (1.78 \times 1) + (2.11 \times 1) + (0.51 \times 1) + (1.87 \times 1) + (0.56 \times 1) + (0.0 \times 1) / 9 \\ &= (2.3 + 2.10 + 1.29 + 1.78 + 2.11 + 0.51 + 1.87 + 0.56) / 9 \\ &= (12.52) / 9 \\ &= 1.39 \end{aligned}$$

The values of the calculated risk i.e. RF (1.39) was compared with the threshold values, as specified in the RAF. The value of the RF is at the high risk as specified in RAF. This value is not tolerable at any cost. Hence, requirement engineers should revise the SRS by incorporating the security related points. We have been replied by the SRS provider that the security feature incorporation has been inadequate in this particular SRS. This replied fact further validates our above mentioned results.

VI. CONCLUSION AND FUTURE WORK

The proposed framework, RAF may be used for the risk assessment as a quantitative measure for the requirements phase of SDLC. Once, the final value of the risk factor is calculated, its tolerance level should be checked. This tolerance level may depend upon the nature of the project. Accordingly, three levels of risks e.g. high, medium, low may be fixed. RAF is validated on a live SRS which reveals that SRS lacks in incorporating security features and needs major modifications with this point of view. There are a number of security loopholes in both the SRS. The requirement engineers should revise the SRS documents and they should add the security flavor before proceeding to the design phase for building secure software which is the thrust area for the customers as well as industry.

Although RAF is validated on one SRS of live project; however, to generalize the results, further study on a large sample of SRS is needed. A software tool may also be developed for the automation of this complete process. In future, depending upon the need of the project and advancement in technology, some more policies may also be added. This work may also be extended for the further phases of SDLC by developing various checklists as per requirement and chaining with requirement phase policies. The work will provide guidance and help to the researchers and industry persons for developing secure software.

VII. ACKNOWLEDGEMENT

The checklists of different policies are adapted by the unpublished project report, submitted to DIT, Ministry of Communications and IT, Govt. of India.

VIII. REFERENCES

[1] Abdullah Tahir, Mateen Ahmed, Sattar Ahsan Raza, Mustafa Tasleem. (2010). Risk analysis of various phases of software development models, European Journal of Scientific Research, ISSN 1450, 140(3), 369-376.

[2] Allen Julia, H. Barnum, Sean Ellison, Robert J., McGraw Gary, Mead Nancy R. (2008). Software security engineering: A guide for project managers. (pp. 6-8). Addison Wesley Professional.

[3] Ashbaugh Douglas A. (2008, October, 23). Security software development, assessing and managing security risk. CRC Press.

[4] Computer Technology Documentation Project. (2009, January). Computer security policy categories and types. Retrieved from January 15, 2009 from http://www.comptechdoc.org/independent/security/recommendations/secpolgen.html

[5] Hirsch Corey & Ezingeard Jean- Noel. (2008, January). Perceptual and cultural aspects of risk management alignment: a case study. Journal of Information Systems Security, JISSec, 4(1), 3-20.

[6] Mccullgh Adrian & Caelli William. (2000, August 7). Non repudiation in the digital environment. First Monday, 5(8). Retrieved May 3, 2008 from http://www.firstmonday.org/issues/issue5_8/mccullagh/

[7] Mazumdar Chandan, Barik Mridul Sankar, Sengupta Anirban. (2007, September). Enterprise information security risk analysis: A quantitative methodology. In the Proceedings of the National Workshop on Software Security. (pp. 1-12). N. Delhi, India.

[8] Mustafa K., Pandey S. K., Rehman S. (2008, September). Security assurance by efficient access control and rights. CSI Communication, 32(6), 29-33.

[9] Mustafa K., Rehman S., Pandey S.K. (2009, March): Confidentiality related security assessments. IEEE International Advance Computing Conference. Patiala.

[10] Mustafa K. & Pandey S. K. (2010, January). A comparative study of risk assessment methodologies. International Journal of Computer Science and Information Security. (Accepted)

[11] National Thermal Power Corporation Ltd. (2006, July). Information security policies & procedures. [Technical report] Final V. 1.0.

[12] Pandey S.K., Mustafa K., Ahson S. I.(2007, December). A checklist based approach for the mitigation of stack overflow attacks. In the Proceedings of the Third IEEE International Conference on Wireless Communications and Sensor Networks, WCSN 2007, (pp. 174-176). Allahabad, India.

[13] Pandey S. K., Mustafa K. (2010, July). Recent Advances in SRE Research. International Journal of Computer Science and Engineering, 2(4), 1079-1085.

[14] Pandey S. K., Mustafa K. (2010, Aug). Security Assurance: An Authentication Initiative by Checklist. International Journal of Advanced Research in Computer Science, 1(2), 110-113.

[15] Stoneburner Gary, Goguen Alice, Feringa Alexis. (2002, July). Risk management guide for information technology systems. NIST Special Publication, (800-30). Retrieved February 14, 2008, from http://csrc.nist.gov/publications/nis tpubs/800-30/sp800-30.pdf