International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-3, February 2019

Implementation of KSM Model to Reduce Software Risks

LellaKranthi Kumar, ParvataneniGeethika, Sriram Konduru,

Abstract: ***This paper deals with the risk management with the help of a certain case study and we propose a KSM model approach for our paper to be implemented for better results and lessen the risk of the system as much as possible. This also helps us in the estimating of the cost effective measures and less uncertain situations in the scenario. This is quite helpful for the risk calculation and estimation along with the avoiding of the risks factored to occur in the process.***

Keywords: Risk management, KSM model approach, estimations, risk analysis, risk calculation.

I.INTRODUCTION:

This shows brief information regarding proposed KSM model, it is a mathematically illustration model that represents numerical values in investigation process of the web based information systems, this model recognize efficiency with respect to the effort and identify the impact of the risk it shows in figure 4.1, this model approach concerns the security risk requirements of the "ISO - IEC 27002" information systems risk management standards[7]. Basically the proposed model has amulti layer structure and each layer have multi levels it based on hierarchical design of the "ISO - IEC 27002" standards. It is hybrid technique that enables both qualitative and quantitative approaches and it enables the low level risk values into upper level risk values[8].

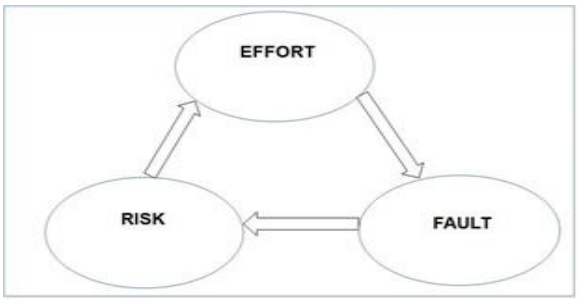

Figure 4.1 Cyclic Process relation between Effort- Fault-Risk

The proposed KSM model has two basic steps follow finalized the risk impact, that ability to confine the people perception and source code analysis use for the effectively in risk management process[9].

Manuscript published on 28 February 2019.
* Correspondence Author (s)
Mr. Lella Kranthi Kumar, Asst. Professor, Dept. of CSE, Lakireddy Bali Reddy College of Engineering,
Parvataneni Geethika, Student in Department of CSE, Lakireddy Bali Reddy College of Engineering,
Sriram Konduru, Student in Department of CSE, Lakireddy Bali Reddy College of Engineering.

The KSM model creates a base for investigation form to collect input data and it shows how mathematical analysis perform for the investigated input data for compute the risk value and their impact. In this paper contribute in addressing of the web based information systems application security readiness by using an effort analyzing, this model is the valid and reliable technique and it follow international standards.

Indicator	TA	PA	D
Development Process			
Experience on the development process	4	1	0
Geographical distribution level	3	2	0
Development System			
Development infrastructure availability	4	1	0
Development software availability	4	0	1
Management Process			
Project manager experience level on managing	4	1	0
Project dependence level	4	1	0
Process changes	3	1	1
Maturity level	4	0	1
Management Methods			
Motivation level	4	1	0
Role organization effectiveness	4	1	0
Work Environment			
Conflict Level	3	1	1
Team Focus	5	0	0
Turnover	4	1	0

Fig_1: Defining the risk levels example

Literature survey:

Information systems risk examination Parker and Fisher have used risk analysis as a essential basis for security blueprint in data systems [1]. They gift general checklists for concerns within the sanctuary assessment. The quandary with precise tools and checklists is that they befall obsolete quickly and wish to be persistently updated [3]. Applications of such equipment don't result in knowledge domain encroachment for data security intend. Backhouse and Dillon (1996) conceive to craft a logical model for data security as a structure of answerability and duty moderately than normal checklists. Anderson, Longley and Kwok (1994) propose a model supported the credentials and cost accounting of bullying originating from the equipped environment and systems that property underneath fortification meet. SuhANd Han (2003) close to an loom for data security risk examination that comes with equipped stability.

They decide the value of assets supported the magnitude of trade functions and therefore the criticality of chattels to operations. Many methodologies [8] area unit utilized in the scrutiny: paired judgment, asset-function obligation tables, and plus desire diagrams[10]. Different models for so as security style what is more specialize in discovery and valuation of system vulnerabilities and pattern of countermeasures (Weiss, 1991).

Author	Purpose	Data collection method	Ranking method
Chan *et al.* [22]	Produce a list of ranked risks in construction project.	Survey	Descriptive statistics, Kendall's concordance test, Spearman's rank correlation test, Mann-Whitney U test.
Karim *et al.* [23]	Determine significant risk factors.	Survey	Frequency of response.
Lam [15]	List of lessons learned.	Case study	Literature review.
Lam *et al.* [24]	Methods on the allocation of risk.	Survey	Fuzzy set theory.
Rezakhani [25]	Classifying risk factors.	Literature review	Constructed a risk breakdown structure.
Zou *et al.* [11]	Determine significance of risk in relation to project objectives.	Survey	Formula based on product between likelihood and impact.

Fig_2: Literature review

Assessing using International standards for WBIS Risks

Any software developed organization trying to get ISO - IEC information systems security and risk free certification, this certificate promotes their information systems and organization vision and mission clearly specify, it should usually move across three successive phases as follows:

- The initial phase is denotes the KSM model gives idea about the configuration of the Software organizations security based risk management system and considers the ISO - IEC standard.
- The second phase is configuring with the international standard requirements, which logically involves the software organizations to implement risk management system using ISO - IEC 27001 and ISO - IEC 27002 standards. Follow the international standards rules and regulations, the software organization assets internally that its RM systems are amenable with the standard, but there is no proof to show procedure.
- The final phase is to get a formal certification of the software company's RMS against ISO-IEC standards by a recognized certification body.

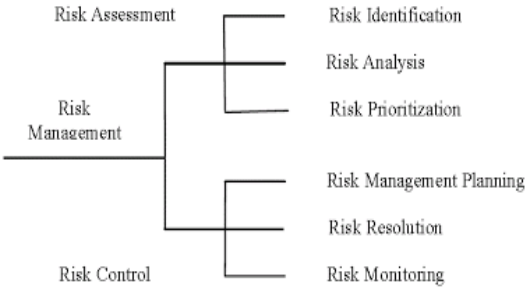

Fig_3: Phases of risk management

According to international standard measurements suggested the following basic steps for the designing and construction of a Risk Management System[11].

- Identify and Developing indicators to measure risk.
- Implement and identify an information system security risk management procedure effectively.
- Collected input data can be integrating and analyzing data.
- Calculate risk using measures which are gather input data from thorough investigation and source code analysis.
- Communicate risk value to the relevant category of the people;
- Based on investigation data computed results as contributing risk factor to RMS-related decisions.

II.MARKOV MODEL

The future development time "t+1" for any process depends at time "t" on the process state, and does not depend on past development at times "t – 1", "t – 2", . . . , "2", "1", "0". We can describe is as follows: for all t = "0", "1", "2", . . . and all states "I", "j", "i_t−1", . . . , $i_0 \in E$ is

$$P(X_{t+1} = j | X_t = i, X_{t-1} = i_{t-1}, \ldots, X_0 = i_0) = P(X_{t+1} = j | X_t = i)$$

These kind of processes are called as the markov chain.

Now we incorporate a new equation which is as follows

$$p_{ij}(t, t+1) = P(X_{t+1} = j | X_t = i)$$

$$p_{ij}(t, t+s) = P(X_{t+s} = j | X_t = i)$$

These are well known as the transaction probabilities but the key note is that they do not depend on their parameter values.

$p_i(0) = P(X(0) = i)$	initial probability of state i,
$\mathbf{p}(0) = (p_1(0), p_2(0), \ldots, p_N(0))$	initial distribution of Markov chain states,
$p_i(t) = P(X(t) = i)$	absolute probability of state i at time t,
$\mathbf{p}(t) = (p_1(t), p_2(t), \ldots, p_N(t))$	absolute distribution of Markov chain states at time t.

With all these we measure up the chain's stationary distribution which has to be probabilistic one.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

If and only iff all the probabilities are said and proved to be stationary then we can call it as an equilibrium (statistic).

Proposed KSM Model Process:

The following figure 4.5 shows the KSM Risk management architecture and it gives detail flow of the KSM model and their process.

Step1: Entire application (i.e. Information System) is divided into fourmodules (People, Organization, Environment, and Technology), each module work as a domain. Mapping the ISO - IEC over the POET domains
Step2: Each Module programs read as input individually and consider effortof the each interface of the product through acquisition process.
Step3: Each individual program effort calculated based on the source codeand it is also module wise i.e., POET.
Step4: consider 75% of the Step3 result and 25% of the Step2 result.
Step5: Estimate the each Module fault based on the effort analysis
Step6: Estimate based on the fault identifies the induced and inherent risks.
Step7: Based on the Step3 and Step4 find out the Risk factor
Step8: Repeat the above step for all modules in the system
Step9: Estimate the individual domain structure risk value.
Step10: Based on the Step 9 to display module risk value and give suggestionsto develop healthy system.

III.RESULTS

Consider another web application like attendance automation system, apply the proposed KSM model the below figure shows the risk evaluation of the given application.

	Technology	organization	people	Environment
KSM	0.790272485	0.883746712	1.105806124	1.105814827
Markov	0.187171742	0.190583795	0.311120927	0.31112349

Table 1: Result analysis

The above results show the proposed model targeting safety issues and using real-life industrial data, based on the result recover the product efficiency very easy.

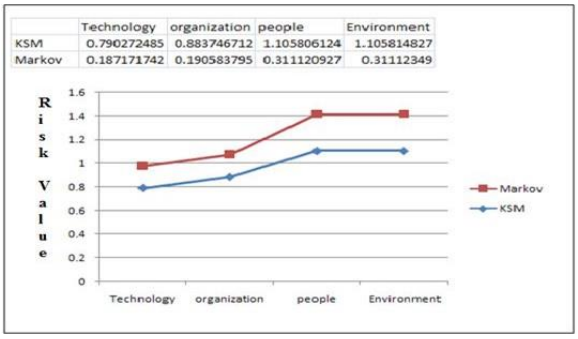

Figure 5. stacked line chart for Combination of ASP and HTML Application

IV.DISCUSSION:

Risk mitigation plays a vital role in success of any software product. Risk mitigation strategies are off four type's i.e. Risk acceptance, Risk Avoidances, Risk limitations, Risk Transmission. Risk mitigation option is always user choice only because the need of the user at present working conditions decides the risk mitigation process consider or not. This process includes lot of money, tike, and man power. So in this KSM model after identification risks according to the domains user need to go risk mitigation process it give suggestions how to avoid impact of the risks with respect of source code design principles. In appendix – II gives brief description about source code analysis with respect to risk impact, and cost. Consider the suggestions user can consternate in the particular discipline and redesigning of code and reduce impact of the risk [3].

V.CONCLUSION

This illustrates illustrates how experimental evaluation is going on with respect to the POET domains and shows the efficiency of the proposed model. In this KSM approach how data collected to evaluate with respect to international standards for the given application is clearly shows. This KSM approach considers only real-life opinions and industrial data only it indicates maintaining of the standards.

REFERENCES:

1. Flanders, W., On the relationship of sufficient component cause models with potential outcome (counterfactual) models. European journal of Epidemiology, 2006, 21(12): p. 847-853.
2. Fenz, S., Pruchner, T. and Manutscheri, A. (2009) Ontological Mapping of Information Security Best-Practice Guidelines. BIS 2009, LNBIP 21, pp. 49-60.
3. FIPS PUB 65, National Bureau of Standards (1997). Guidelines of Automatic Data Processing Risk Analysis. USA: Washington D.C., General Printing Office.
4. Fulford, H. and Doherty, N. (2003) The application of information security policies in large UK-based organizations: an exploratory investigation. Information Management & Computer Security, 11(3), pp. 106-114.
5. Fung, A. R., Farn, K. and Lin, A. (2003) A study on the certification of the information security management systems. Computer Standards & Interfaces, 25(5), pp. 447-461.
6. Summit in Okinawa, Japan (July 2000) [online]. Available from: http://www.g7.utoronto.ca/summit/2000okinawa/gis.htm [Accessed: 25 May 2007].
7. Devanbu, P.; Fong, P.W.-L.;Stubblebine, S.G. (1998) Techniques for trusted software engineering. Proceedings of the 1998 International Conference on Software Engineering, pp. 126–135
8. Rabiner, L. R. (1989). A tutorial on hidden Markov models and selected applications in speech recognition, Proceedings of the IEEE, 77 (2), 257-286.
9. Chittister, C. and Haimes, Y.Y., Assessment and Management of Software Technical Risk, IEEE Transaction on Systems, Man, and Cybernetics, vol. 24, no. 2, Feb., 1994.
10. Greer, D., Report on SERUM trial at NEC Corp., University of Ulster, 1998.
11. Greer, D. and Bustard, D.W., SERUM-Software Engineering Risk: Understanding and Management, The International Journal of Project & Business Risk, vol. 1, Issue 4, winter, pp. 373-388, Project Manager Today Publications, 1997(2).

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

AUTHORS PROFILE

Lella Kranthi Kumar, Currently working as an Assistant Professor in the Department of Computer Science and Engineering in Lakireddy Bali Reddy College of Engineering, Mylavaram, Krishna District, Andhra Pradesh, India. I am an enthusiast of learning new things and applying that knowledge for solving real-world problems. I am a proud tech-savvy, who is keen about all the tech stuff happening around the globe. I am not like a nerd but socially conscious about everything happens around me and take the decisions wisely and politely without hurting others opinions. This is the main reason that my research interests are mainly focused on Education Technologies, especially about "Online based blended Teaching-Learning process" that effectively uses current network infrastructure perfectly and makes the process of learning easy to all sort of people around the globe. In addition to the above, my research interests go on Data Analytics, IoT and Medical Image Processing.

Parvataneni Geethika, currently a student of Computer Science and Engineering in Lakireddy Bali Reddy College of Engineering, Mylavaram, Krishna District, Andhra Pradesh, India. I am an enthusiast of learning new things and applying that knowledge for solving real-world problems. I am a proud tech-savvy, who is keen about all the tech stuff happening around the globe. I am not like a nerd but socially conscious about everything happens around me and take the decisions wisely and politely without hurting others opinions.

Sriram Konduru, currently a student of computer science and engineering in Lakireddy Bali Reddy College of Engineering, Mylavaram, Krishna District, Andhra Pradesh. I am an active learning who likes to know more about things irrespective of domains and subject restrictions. I am always eager to compete in a healthy competitive environment. I look forward to sharpen my skills and learn much more to attain even more knowledge for which I'm greedy in a positive sense. I look forward in meeting new people as I can and will learn something from each and every person I meet. Finally I want all this knowledge to be useful for the betterment of the society and my surroundings. I like my work to be useful for mankind and benefit in the betterment of our daily life.