International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-6, March 2020

Analyzing and Managing the Impact of Risks using Multi Fuzzy Inference System

Malaya K Nayak, Arka K. Das Mohapatra

Abstract: ***Information technology security risk evaluations are necessary in determining measures being taken for risk analysis. Risk analysis is also significant as it predicts the loopholes in the software which can get manipulated during suspicious activities. The article has attempted to analyze the risk issue and further suggests a multi-fuzzy risk evaluation approach for the identification of security threats. This approach analyses hacker risks based on the potential ability for an assailant, their overall probability for an attacks as well as the implications of such attacks. It typically consists of 3 sub fuzzy inference structures. The 1st fuzzy inference structure assesses an assailant's total capacities. The 2nd fuzzy inference structure assesses the general probability of ambush success, whereas the 3rd fuzzy inference structure measures risk thresholds.***

Keywords: IT Risks, project risk management, fuzzy interference system, risk evaluation, project management.

I. INTRODUCTION

The comprehensive risk analysis and assessment estimates can provide profitable support for decision-making (NIST, 2012). This can be a very simple process established on well-known reasoning as well as in the right direction. Such approaches are descriptive, quantitative and semi-quantitative (NIST, 2011), owing to the available data as well as the degree of necessary details (Zirakja and Samizadeh, 2011). Procedures for risk examination are receptive to the idea to monitor uncertainties. Quantitative risk analysis encompasses the quantitative perspective of achievement probabilities and outcomes for a mathematical risk evaluation. There is a whole range of commonly used risk analysis methods which, aim to determine and predict threats. Quantitative strategies are used for quantitative processes, for example, fault and activity decision tree analyses, Monte Carlo computation, susceptibility analysis, yearly loss expectations, potential losses, fail sequence as well as implications evaluation. Qualitative procedures may be more based on assessment than statistics like hypothetical situation evaluation. Semi quantitative would be an intermediary technical procedure in which there are no limited or obvious threats and several complicated risks including advanced processes or techniques; a basic empirical methodology could be complemented with such a semi-quantitative analysis.

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author
Dr. Malaya Kumar Nayak, Director, IT Buzz Ltd and U-Com Software Private Ltd, Satya Nagar, Bhubaneswar, India.
Prof. Dr. A. K. Das Mohapatra, Professor, Department of Business Administration, Sambalpur University, Odisha, India.

There are key elements and drawbacks in qualitative and quantitative methods. This kind of appraisal will gain from objective and subjective assessments (NIST, 2012). Several specific procedures for conducting semi quantitative risk assessments exist, quantifying approaches to potentially harmful structure and routes of project defensive layer assessments.

The use of the Fuzzy Inference System (FIS) for fortuitous investigation is also one of many such approaches and the analysis is extremely subjective as well as may relate to unreliable and vague data (Zirakja and Samizadeh, 2011). Conceptual principles for theoretical logic have already been commonly seen when FIS was first developed to address issues of ambiguity by Lotfy Zadeh (1965). A principle-based, fuzzy analyst analysis software application has also been used to assess the product danger prior to its eventual deployment (Sodiya, Longe and Fasan, 2007). The framework provided in the work of Choudhary and Raghuvanshi (2012) to facilitate the evaluation of risk analysis for governmental institutions throughout the domain of data securities. This article uses a Multi Fuzzy Inference System MFIS (MFIS) developed to evaluate the threat frequency through utilization of possible risk-related parameters. Fuzzy inference is a programming model containing a set of fluidity features, laws including reasons for inclusion. We use the Mamdani Fuzzy paradigm, so that we can best customize our method (Sonia, Singhal and Banati, 2011) using MFIS strategy.

II. EVALUATION METHODS

In developing and implementing efficient data/project security programs, risk management has a crucial role as well as enables organizations to resolve a variety of security-related problems owing to complex recurrent threats related to project management issues. The evaluation of potential safety risks requires a proper review of details regarding risks and weaknesses to evaluate to what degree conditions or incidents can have an adverse effect on an enterprise as well as the probability of accidents and situations NIST(2012). Risk assessment is indeed the mechanism by which the risks of projects and data securities are identified, prioritized as well as estimated NIST(2012). Institutions have used the outcomes of risk analysis to establish relevant alternatives which can deliver successful risk reactions and measures as part of a comprehensive risk assessment mechanism. Figure 1 represents a model flow diagram of steps involved in risk evaluation. Usually, every risk analysis requires:

1. An indirect risk prototype that sets out key concepts, evaluable risk parameters, as well as interrelationships.

2. An appraisal method to identify the set of parameters that these risk parameters will carry on throughout the test.
3. A tool to analyze how well these variables' meanings are systematically coupled with a risk assessment framework.

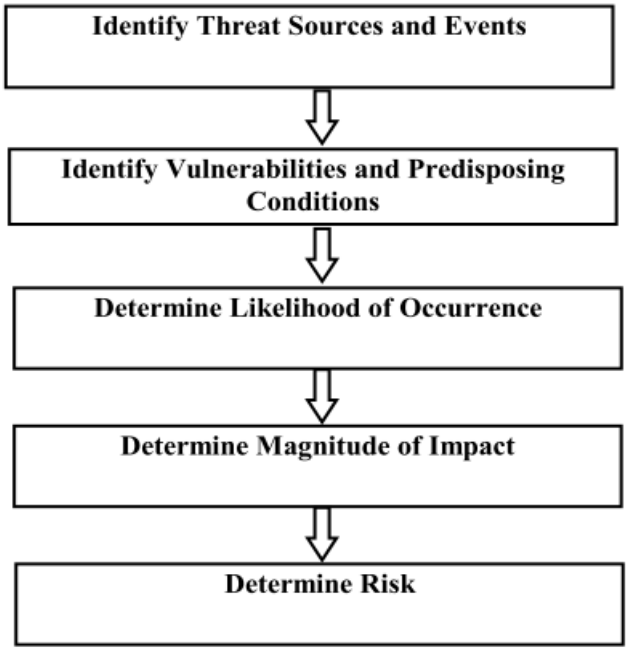

Fig. 1.Steps for risk evaluation

Risk assessments address the potential adverse impacts to organizational operations and assets, individuals, other organizations, arising from the operation and use of information systems and the information processed, stored, and transmitted by those systems. Risk evaluations aren't just one-time operations that provide policy-makers with durable or concrete details for guiding and advising data security and risk behaviors NIST,(2011). Evaluation of risks can be performed using the proposed equations:

Risk=(impact x overall capabilities x overall likelihood) (1)
Overall-likelihood=(V x A x S) (2)
Overall capabilities=(target x intent x capabilities) (3)

where *V* represents vulnerability, S represents likelihood success, as well as *A* represents likelihood activity.

Informative vulnerabilities represent possible negative consequences for organization's activity (i.e. project, working, appearance or prestige), organizational property, persons, and others, resulting from classified loss, integrity or access to information or information systems.

III. RISK MODEL

This includes identification and threat categorization for each resource or element, risk ranking oriented threats, therefore the development of risk mitigation measures which will then become enforced throughout the development process. The main property of installation must be identified with potential program break-down threats. The simulation of the risks is the approach by which a software defines, quantifies as well as analyses possible system threats. Moreover, modelling of risks attacks is a popular and successful implementation. A variety of risk assessment management priority systems exist in open-source.

Risk modeling describes the risk parameters as well as the connections between them. Risk parameters are features that can be used in risk designs as input and output in risk management for determining risk levels NIST(2012). Risk and threat incident, weakness, influence, probability, vulnerability, and susceptibility situation, as demonstrated in Figure 2, involve standard risk parameters. Risk parameters could be broken down further into comprehensive attributes (for example, the threats could be broken-down into origins of risk and real danger).

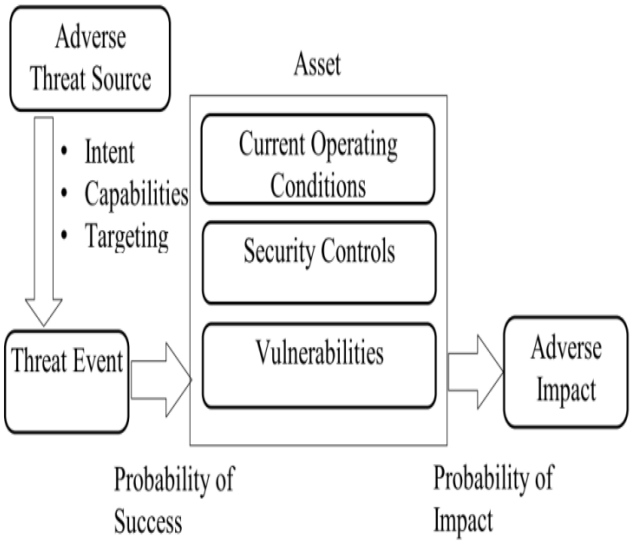

Fig. 2.Model for assessment of risks

A. Risk Factors

(i) ***Threat*:** Risk to organizational activities and properties, persons, other entities or the government via data systems, through security breaches, degradation, leakage or alteration of data or by refusing a service, or via a threat to humanity, would be any situation or occurrence which is potentially unfavorable (U.S. Department of Energy,2012). Digital threats against a monitoring system include individuals that try unauthorized use of a data exchange routes to access to a computer-controlled device or otherwise connection interface.

(ii) ***Vulnerability:*** a vulnerability is the shortcoming of a risk-source data management, safety protocols, risk management, or framework.

(iii) ***Probability:*** a measured potential risk seems to be the possibility of a risk which is focused onto an estimation of the probabilities that somehow the risk will leverage the flaws (or vulnerabilities) NIST (Feb. 2006).

(iv) ***Impact:*** The degree of effect of a vulnerability is the extent to which the unauthorized divulgation of data, unauthorized modifications of data, unauthorized degradation of data or lack of data or by the provision of data technology could be known as intended results. Technical, social and economic effects may be affected Wonder ware Invensys Systems,(2007).

Figure 3 below depicts interconnective flow of various malicious risk factors.

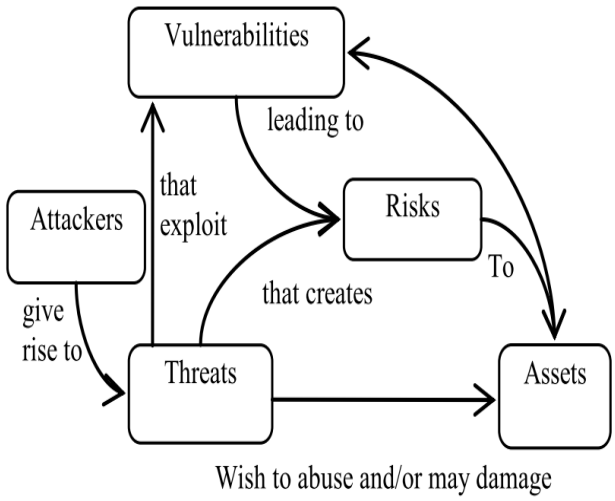

Fig. 3.Flow of malicious acts

Proposed Multifuzzy Inference System (MFIS)

We have been suggesting MFIS approach focused on the IT risk paradigm as reflected by Equations-1, 2 and 3, consisting of 3 quizzical risk evaluation interpretation structures as can be seen in Figure 4. The 1st FIS-1 computes the total capacity (abilities, purpose as well as target), as it is used in a risk point of origin including a terrorist or rebel group. The FIS-2 measures the average probability for an undesirable risk activity depending on assorted risk variables (exploitable flaws, the probability of intervention as well as the level of risk). The FIS-3 computes the hazard level on the basis of the performance of FIS-1, FIS-3 as well as the inverse effects. The descriptive agreement conditions for all fuzzy factors are: Ability, goal, aim, uncertainty, threat, probability of intervention, performance potential, effect as well as threat rate defined as, "__Very low'', "__low'', "__Moderate'', "__High'', and "__Very High'' (see Table 1 and Figure 5). In the whole research paper, the semantic member functionalities were characterized by triangular affiliation for "very low and very high" and angular member-ship functionalities in "low," and "moderate" since these are frequently applied in programs like fluids as well as administrative decision-makings (Table 2).

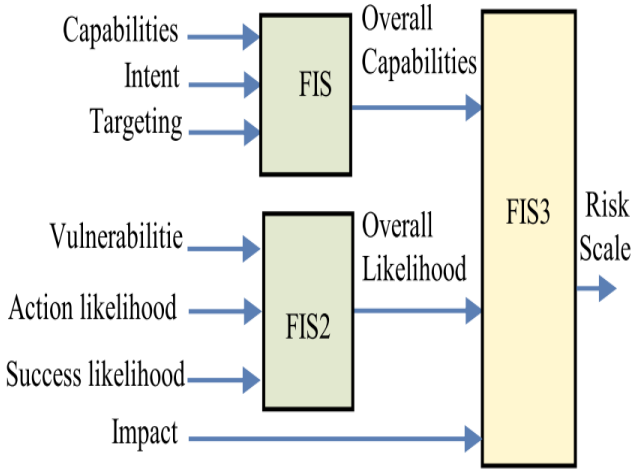

Fig. 4.Proposed MFIS system

Table-II.Adversary Capability (adapted from NIST,(2012))

Fuzzy Sets	Meaning
Very high	Extreme high risks suggest that perhaps a risk incident may have several serious or devastating harmful impacts.
High	High risk indicates a harmful or fatal negative impact can be anticipated.
Moderate	A medium risk can result in a major negative impact of a threat incident.
Low	Moderate risks can lead to a major negative impacts for a risk incident.
Very low	Very low risks mean that perhaps the marginal negative impact of a risk incident may be anticipated.

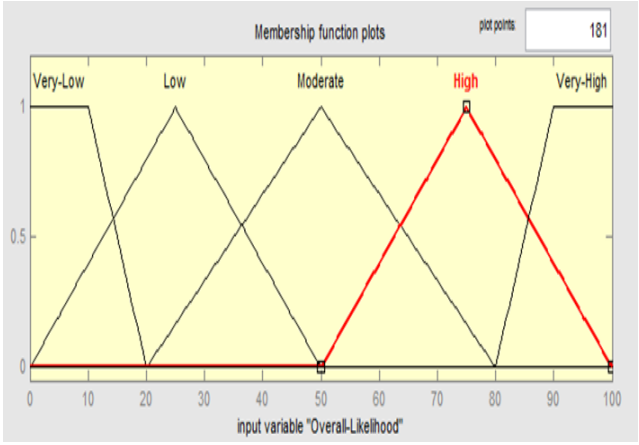

Fig. 5.Fuzzy Sets

Table-II.Probability of Risk Incident triggers NIST, (2012))

Fuzzy Sets	Meaning
Very Low	The enemy seems to have very limited funds, skills or prospects to encourage major attacks.
Low	The enemy acquires very limited capability, skills as well as the potential for major attacks.
Moderate	The opposing party has reasonable capital, knowledge or resources for attempted attacks.
High	The attacker seems to have a high degree of competence as well as considerable wealth including potential to fund many simultaneous attacks effectively.
Very High	The attacker may have very advanced knowledge and skills, is also well equipped to provide the potentials for many popular, unresolved and organized threats.

A. Implementation of MFIS

We have implemented our method using Matlab fuzzy toolbox. The FIS editor of fuzzy toolbox is used to define input, output names for FIS-1, FIS-2, and FIS-3. Also to specify, the fuzzy operations such as AND (*min*), and OR (*Max*), and methods used to define Implication (*min*),

Aggregation (*max*), and Defuzzification (*centroid*). After that the rule editor of FIS is used to edit, add, delete or change a rule. FIS editor can also be used to change the connection type (AND, OR) and the weight (importance) of a rule, the default value is 1. The rule editor for FIS-3 with input output settings is shown Figure 6 where all the rules have the same importance (*i.e. weight=1*).

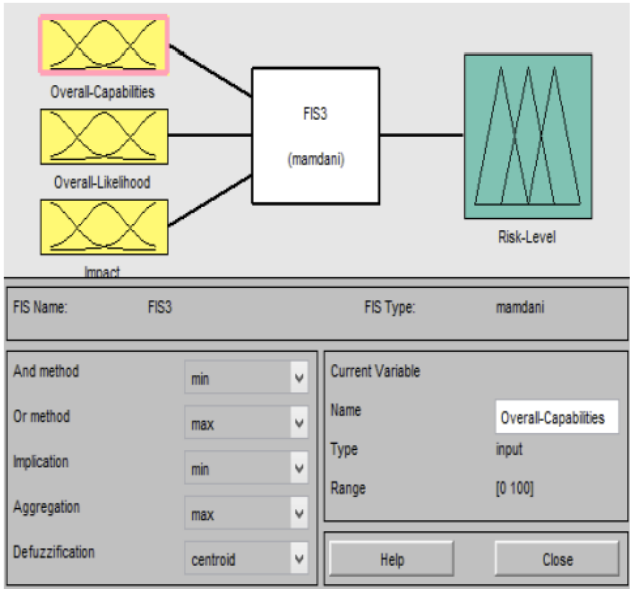

Fig. 6.FIS-3 Inputs, Output, and Setting Parameters

B. Rule Viewer

A graphic display of parameters via overall criteria can be seen in the standards display (Figure 7), which reflects the mixture of both the principles as well as the effect of de-fuzzification. The machine performance is however shown as a clear quality. For the analytical study, data should be inserted through the text inputs via the Rule Viewer. The discharged regulations as well as fuzzy collections were shown on the screen with rules as per the data inputs.

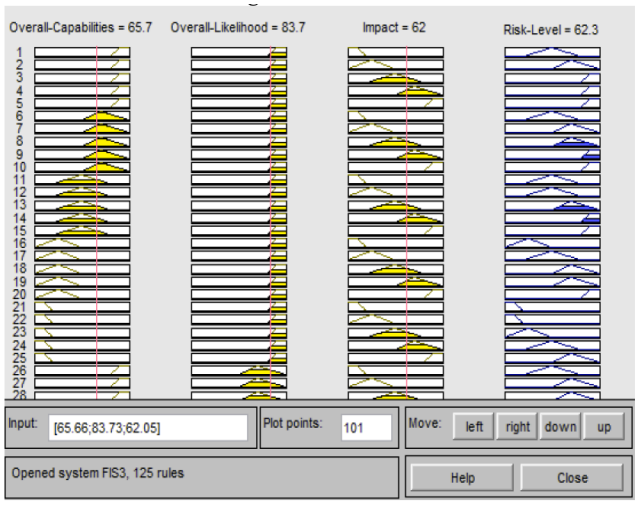

Fig. 7.Rule Viewer

The relative risk rating, for instance, as can be seen in Figure 7 with total of 65.7 input sources, 83.7 comprehensive risks, as well as 62 effects, results in 63.8 outputs. A 3D graph illustrates the connection among inputs and outputs in the FIS's interface window. Here demonstrated in Figure 8, the result, the threat degree of the z-axis can be seen, whereas, two factors can be seen, influence on x-axis as well as total potential on y-axis, and effects on x-axis or even total probability on y-axis. The surface monitor displays a map of potential outputs from the available input levels.

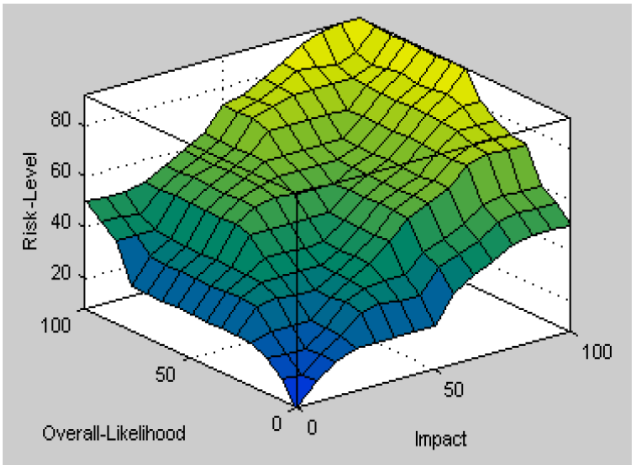

Fig. 8.Surface Viewer for (likelihood, impact, and risk level)

C. Evaluation

In order to determine various hacker-threat situations and therefore reconsider updates or using more security protocols to minimize project risks, the suggested risk analysis approach could be utilized. The approach suggested could be utilized to design numerous sources of risk like militants, radicals, irritated staff, undercover operatives including terrorist organizations with varying capacities, motives as well as targets (Table 3).

Table-III.Risk Assessment Results

Total hacker capacity	91
Total probability of success	90
Impacts	89
Risk levels	91

As somewhat of a test case, attackers could use these details to acquire nuclear material that can be used for nasty pumps through obtaining confidential information regarding the current shipment of nuclear materials stored in the data systems. The measurement results as represented in Table 3, the industry's shortcomings are vulnerable safety checks as well as the environment of protection, Internet service including poor personal safety of staff is deep. Whereas, a programmer with extensive knowledge can hack control system databases according to various flaws. The latter's intention would be to steal data connected to transporting goods of nuclear materials as well as acquire it for militants to even get profit, although it is strongly successful, there is still a very good possibility of a terrorist organization attempting to steal fissile materials and the threat of terrorist groups who use such nuclear materials in filthy displays.

IV. CONCLUSION

This study introduces a new way to evaluate IT-based safety risks using MFIS. The approach presented is dependent on the latest threat framework that considers most risk parameters including framework flaws, the probability of exploitation as well as the risks of failure. In comparison to the pervasive risk framework, practical modelling of the process setting reflects just the probability for an occurrence as well as its effects. The 1st fuzzy FIS-1 exemption model calculates the aggregate risk origin capacity for an attacking asset (capability, intention as well as targeted) as more of an insurgent group or even a hacking team. The 2nd FIS-2 method measures the general possibility of risk consequences on the basis of risk parameters (vulnerability, possibility of intervention, and probability of successes). FIS-3 determines the risk changes depending on the throughput of FIS-1 and FIS-3 as well as their combined effects and adverse influences. The use presented approach could be utilised to evaluate the risk of security threats towards any program.

REFERENCES

1. M.H. Zirakja, R. Samizadeh,-Risk Analysis in E-commerce via Fuzzy Logic, Int. J. Manag. Bus. Res., 1 (3), 99-112, summer 2011.
2. National Institute of Standards and Technology NIST (Feb. 2006), Guide for Developing Security Plans for Federal Information Systems.
3. National Institute of Standards and Technology NIST (Feb. 2012), Framework for Improving Critical Infrastructure Cyber security, Version 1.0.
4. National Institute of Standards and Technology NIST Special Publication 800-39, March 2011, Joint Task Force Transformation Initiative, Managing Information Security Risk: Organization, Mission, and Information System View.
5. National Institute of Standards and Technology NIST Special Publication 800-30 rev. 1 (Sep. 2012), Guide for Conducting Risk Assessments.
6. Rahul Choudhary and Abhishek Raghuvanshi,-Fuzzy Based Evaluation Model of a Systems Security, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 9, September 2012.
7. Sodiya, A.S., Longe, H.O.D. and Fasan, O.M., -Software Security Risk Analysis using Fuzzy Expert System, In Journal of INFOCOMP: Journal of Computer Science, Brazil, Vol. 7, No. 3, 70-77, 2007.
8. Sonia, A. Singhal, H. Banati,-Fuzzy Logic Approach for Threat Prioritization in Agile Security Framework using DREAD model,. In IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No. 1, July 2011, Mauritius.
9. U.S. Department of Energy, Electricity Subsector Cyber security Risk Management Process, DOE/OE-0003, May 2012.
10. Wonderware Invensys Systems, Inc Revision 1.4, (2007), Securing Industrial Control Systems, A guide for properly securing Industrial Control Systems operating in a Microsoft Windows environment.
11. Zadeh, L. A. -Fuzzy sets. Information and Control, 1965.

AUTHORS PROFILE

Dr. Malaya Kumar Nayak, is an Entrepreneur and researcher with over 23 years leading the design, development and implementation of high-performance Executive Director with IT Buzz Ltd and U-Com Software Private Ltd. He has received M.S degree in ICT from Assumption University and PhD degree in Computer Science from Utkal University. He has published more than 25 research papers in National & International Conferences and Journals. His current research interests in project management and risk management.

Prof. Dr. A.K. Das Mohapatra, is currently a Professor of Business Administration in Sambalpur University, Odisha, India. He has 30 years of teaching, research and consultancy experience to his credit. He has authored 7 books including International Accounting published by PHI. He has also published over 85 researh papers in the field of Accounting, Finance, Strategic Management and Corporate Governance. A Gold Medallist from Utkal University, Bhubanrswar, India, Prof Mohapatra holds a Ph.D in Finance and D.Litt in Management focussed on Corporate Governance.