INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, IT & MANAGEMENT

IJRCM

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A.,

Open J-Gage, India [link of the same is duly available at Inflibnet of University Grants Commission (U.G.C.)],

Index Copernicus Publishers Panel, Poland with IC Value of 5.09 & number of libraries all around the world.

Circulated all over the world & Google has verified that scholars of more than 2980Cities in 165 countries/territories are visiting our journal on regular basis.

Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

http://ijrcm.org.in/

CONTENTS

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the areas of Computer Science & Applications; Commerce; Business; Finance; Marketing; Human Resource Management; General Management; Banking; Economics; Tourism Administration & Management; Education; Law; Library & Information Science; Defence & Strategic Studies; Electronic Science; Corporate Governance; Industrial Relations; and emerging paradigms in allied subjects like Accounting; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Rural Economics; Co-operation; Demography: Development Planning; Development Studies; Applied Economics; Development Economics; Business Economics; Monetary Policy; Public Policy Economics; Real Estate; Regional Economics; Political Science; Continuing Education; Labour Welfare; Philosophy; Psychology; Sociology; Tax Accounting; Advertising & Promotion Management; Management Information Systems (MIS); Business Law; Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labour Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; International Relations; Human Rights & Duties; Public Administration; Population Studies; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism & Hospitality; Transportation Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic; Web Design and emerging paradigms in allied subjects.

Anybody can submit the **soft copy** of unpublished novel; original; empirical and high quality **research work/manuscript** ***anytime*** in ***M.S. Word format*** after preparing the same as per our **GUIDELINES FOR SUBMISSION**; at our email address i.e. infoijrcm@gmail.com or online by clicking the link **online submission** as given on our website (***FOR ONLINE SUBMISSION, CLICK HERE***).

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____

THE EDITOR
IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF.**

(e.g. Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Engineering/Mathematics/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript entitled '_____' for possible publication in your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the author (s) have seen and agreed to the submitted version of the manuscript and their inclusion of name (s) as co-author (s).

Also, if my/our manuscript is accepted, I/We agree to comply with the formalities as given on the website of the journal & you are free to publish our contribution in any of your journals.

NAME OF CORRESPONDING AUTHOR:
Designation:
Affiliation with full address, contact numbers & Pin Code:
Residential address with Pin Code:
Mobile Number (s):
Landline Number (s):
E-mail Address:
Alternate E-mail Address:

NOTES:

a) The whole manuscript is required to be in ***ONE MS WORD FILE*** only (pdf. version is liable to be rejected without any consideration), which will start from the covering letter, inside the manuscript.
b) The sender is required to mentionthe following in the **SUBJECT COLUMN** of the mail:
New Manuscript for Review in the area of (Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/ Engineering/Mathematics/other, please specify)
c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any specific message w.r.t. to the manuscript.
d) The total size of the file containing the manuscript is required to be below **500 KB**.
e) Abstract alone will not be considered for review, and the author is required to submit the complete manuscript in the first instance.
f) The journal gives acknowledgement w.r.t. the receipt of every email and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending separate mail to the journal.

2. **MANUSCRIPT TITLE:** The title of the paper should be in a 12 point Calibri Font. It should be bold typed, centered and fully capitalised.

3. **AUTHOR NAME (S) & AFFILIATIONS:** The author (s) **full name**, **designation**, **affiliation** (s), **address**, **mobile/landline numbers**, and **email/alternate email address** should be in italic & 11-point Calibri Font. It must be centered underneath the title.

4. **ABSTRACT:** Abstract should be in fully italicized text, not exceeding 250 words. The abstract must be informative and explain the background, aims, methods, results & conclusion in a single para. Abbreviations must be mentioned in full.

5. **KEYWORDS:** Abstract must be followed by a list of keywords, subject to the maximum of five. These should be arranged in alphabetic order separated by commas and full stops at the end.

6. **MANUSCRIPT:** Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. It must be prepared on a single space and single column with 1" margin set for top, bottom, left and right. It should be typed in 8 point Calibri Font with page numbers at the bottom and centre of every page. It should be free from grammatical, spelling and punctuation errors and must be thoroughly edited.

7. **HEADINGS:** All the headings should be in a 10 point Calibri Font. These must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.

8. **SUB-HEADINGS:** All the sub-headings should be in a 8 point Calibri Font. These must be bold-faced, aligned left and fully capitalised.

9. **MAIN TEXT:** The main text should follow the following sequence:

INTRODUCTION

REVIEW OF LITERATURE

NEED/IMPORTANCE OF THE STUDY

STATEMENT OF THE PROBLEM

OBJECTIVES

HYPOTHESES

RESEARCH METHODOLOGY

RESULTS & DISCUSSION

FINDINGS

RECOMMENDATIONS/SUGGESTIONS

CONCLUSIONS

SCOPE FOR FURTHER RESEARCH

ACKNOWLEDGMENTS

REFERENCES

APPENDIX/ANNEXURE

It should be in a 8 point Calibri Font, single spaced and justified. The manuscript should preferably not exceed ***5000 WORDS***.

10. **FIGURES &TABLES:** These should be simple, crystal clear, centered, separately numbered & self explained, and **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. It should be ensured that the tables/figures are referred to from the main text.

11. **EQUATIONS:**These should be consecutively numbered in parentheses, horizontally centered with equation number placed at the right.

12. **REFERENCES:** The list of all references should be alphabetically arranged. The author (s) should mention only the actually utilised references in the preparation of manuscript and they are supposed to follow **Harvard Style of Referencing**. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parentheses.
- The location of endnotes within the text should be indicated by superscript numbers.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–22 June.

UNPUBLISHED DISSERTATIONS AND THESES

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Natural Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

AN IMPROVED APPROACH OF RISK ANALYSIS FOR IT & ITES ORGANIZATIONS

CHELLAM SHENBAGAM
IT BUSINESS ANALYST AND PROJECT CONSULTANT
SM ENTERPRISES
MADURAI

ABSTRACT

As most of the service delivery organizations use information technology (IT) systems to process their information for better support of their core business objectives, risk management plays a critical role in protecting an organization's information assets. Various models are being carried out to handle the risks by IT companies. The Risk Management model discussed in this study is a true recognition of the improvised risk management practices leading towards better safer and less hazardous working places in the Industries. Risk management, the process designed to identify critical business functions and workflow, determine the qualitative and quantitative impacts of a disruption, and to prioritize and establish recovery time objectives. Among the important processes of risk management, the risk analysis (determination) process is considered as critical and necessary as the process focus on determination of risks identified within IT systems of organization so that to dimension the need of control plans, risk mitigation process to bring down the risks to acceptable limits of management. This study is to discuss the various challenges faced by ITeS (Information Technology enabled Systems) companies, risks associated with them and the analytic techniques practiced in industries now for risk determination to manage interruption risks. This study concludes with an improved approach for risk analysis arrived based on the inputs of studies undertaken on the risk management practices followed by both IT and ITeS organizations. The improved approach is widely accepted for its effective and efficient way of handling risks pertaining to IT systems. The ultimate goal is to help organizations to better manage IT-related mission risks.

JEL CODE
M49

KEYWORDS
IT, ITeS, FMEA, Risk, Risk Analysis, Risk Management.

INTRODUCTION
The principal goal of an organization's risk management process should be to protect the organization and its ability to perform their pre-established objective, not just its IT assets. Nowadays, Risk Management is also used as a tool identifying business opportunities to design and modify the IT products and solutions. The elementary Risk Audits for System Breakdown failures, Fire Safety, Electrical safety, Comprehensive Safety, Business Interruption Risk Analysis, Flood Risk Management etc has been practiced for the improvements of the Risk level in the organizations. The preventive maintenance, scheduled maintenance in Industries and extensive use of techniques like **FMEA** and Logistic Risk Management with the use of sophisticated instruments like **data logger** has improved the trends of Risk Management to the truly international standard. A successful risk management program will rely on (1) senior management's commitment; (2) the full support and participation of the IT team; (3) the competence of the risk analysis team which must have the expertise to apply the risk determination methodology to a specific site and system, identify mission risks, and provide cost-effective safeguards that meet the needs of the organization; (4) the awareness and cooperation of members of the user community, who must follow procedures and comply with the implemented controls to safeguard the mission of their organization; and (5) an ongoing evaluation and determination of the IT-related mission risks. Based on a comprehensive review of literature and theoretical background of the risk, the suitable risk analysis tool is studied and found as an improved approach than the prevailing practice in IT industries.

LITERATURE REVIEW
a) **QUOTE**

"*Even the basic building design is not very conducive to set up a unit. The structures are not convenient for housing facilities like air conditioning vents, service shafts and other things*" - Nakul Subramanyan, FirstSource's infrastructure and administration vice-president, IT conference, SEZ-India 2008.

b) **UNDERSTANDING RISK, THREAT & VULNERABILITY**

A study by Anadi Kishore Sethi – "The Indian Trends in Risk Management Practices"

- **Risk** is the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence. **Risk** is a function of the **likelihood** of a given **threat-source's** exercising a particular potential **vulnerability**, and the resulting **impact** of that adverse event on the organization.
- **Threat** is the potential for a particular threat-source to successfully exercise a particular vulnerability.
- **Vulnerability** is a weakness that can be accidentally triggered or intentionally exploited. A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised and result in a security breach or a violation of the system's security policy.

c) INSTANCES FOR RISK, THREAT & VULNERABILITY

TABLE 1: VULNERABILITY/THREAT PAIRS

Vulnerability	Threat	Threat Actions
Flaws in the security design of the system; new patches have not been applied to the system	Unauthorized users (e.g., hackers, disgruntled or terminated employees, computer criminals, terrorists)	Obtaining unauthorized access to sensitive system files based on known system vulnerabilities
Data center uses water sprinklers to suppress fire; No tarpaulins to protect hardware and equipment from water damage in case of failed sprinklers	Fire, negligent persons	Water sprinklers being turned on in the data center

d) **RISK MANAGEMENT**

It is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. The objective of performing risk management is to enable the organization to accomplish its mission(s) by

1) better securing the IT systems that store, process, or transmit organizational information;
2) enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget; and
3) assisting management in authorizing (or accrediting) the IT systems on the basis of the supporting documentation resulting from the performance of risk management.

Risk management encompasses the processes: **risk identification, risk assessment**, **risk determination (Analyze), Control Plans, risk mitigation**, and **evaluation & re-assessment**.

i) **Risk Identification** is the process of identifying any real or potential condition that can cause degradation, injury, illness, death or damage to or loss of equipment or property. Experience, common sense, and specific analytical tools help identify risks.

ii) **Risk assessment** is to determine the extent of potential threat and the risk associated with an IT system throughout its SDLC. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process.

iii) **Risk Analysis / Determination:** The purpose of this step is to analyze and assess the level of risk to the IT system. The determination of risk for a particular threat/vulnerability pair can be expressed as a function of

- likelihood of a given threat-source's attempting to exercise a given vulnerability
- magnitude of impact should successfully exercise the vulnerability
- Adequacy of planned or existing security controls for reducing or eliminating risk.

iv) **Control Plans**: Decision-maker must choose the best control or combination of controls, based on the analysis done. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

- Effectiveness of recommended options (e.g., system compatibility)
- Legislation and regulation * Organizational policy
- Operational impact * Safety and reliability.

The control recommendations are the results of the risk analysis process and provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.

v) **Risk mitigation** In prior to Risk mitigation process, the risk analysis report shall need to be generated which helps senior management, the mission owners, make decisions on policy, procedural, budget, and system operational and management changes. It involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk analysis process. Because the elimination of all risk is usually impractical or close to impossible, it is the responsibility of senior management and functional and business managers to use the **least-cost approach** and implement the **most appropriate controls** to decrease mission risk to an acceptable level, with **minimal adverse impact** on the organization's resources and mission. Organizations can analyze the extent of the risk reduction generated by the new or enhanced controls in terms of the reduced threat likelihood or impact. .

vi) **Supervise and Review:** Once controls are in place, the process must be periodically reevaluated to ensure their effectiveness. Workers and managers at every level must fulfill their respective roles to assure that the controls are maintained over time. The risk management process continues throughout the life cycle of the system, mission or activity.

e) **RISK DETERMINATION TECHNIQUES**:

The risk determination is generally achieved by a deterministic and/or a stochastic method. There are techniques that combine the technology and expertise in identifying foreseeable failure modes of service or resource or process for its elimination. These are intended to recognize and evaluate the potential failure and its effects identify actions that could reduce or eliminate the potential failure chances.

STATEMENT OF THE PROBLEM

IT or ITeS organizations often face issues leading to their business interruption mainly due to infrastructure failures or lapses in logistics support. It includes support from own employees or external technical support like service provider, vendors. The key challenges can be classified as below:

Physical infra requisites	Logistics support	Technical support
Δ IT Hardware & Software	Δ Physical security access	Δ Hardware support
Δ AC & Power	Δ Space & Hygiene maintenance	Δ Telecommunication Infrastructure

The above similar challenges provide enough support for the growing ITES industry to pursue their aggressive business development strategy includes **Risk Management.** Some of the ITeS organizations that are the offshoot of Indian IT giants like Infosys, TCS, Wipro, and CTS are already aware of the sophisticated estimation techniques that their parent company has been using to manage their projects. But the other new organizations are yet to understand the significance of risk management process and gain competencies in this area.

NEED AND SIGNIFICANCE OF THE STUDY

It is nowadays essential that there are techniques exist which combines the technology and expertise in identifying foreseeable failure modes of service or resource or process for its elimination and also to protect the organization and its ability to perform their pre-established objective, not just its IT assets. These are intended to a) recognize and evaluate the potential failure and its effects, b) identify actions that could reduce or eliminate the potential failure chances.
In this study, we discuss the improved approach **Risk-Level Matrix** for risk analysis and existing widely used technique **FMEA** in detail to understand the significance of them in risk management.

SCOPE & LIMITATIONS OF THE STUDY

The study is limited to the scope only towards risk management approaches for IT and ITeS organizations as the study considered features of IT products and services alone. At the same time, there were limitations that need to be acknowledged and addressed regarding the present study. The important limitation that has to do with the extent to which the findings can not be generalized beyond the cases studied.

OBJECTIVES OF THE STUDY

a) To explore the risk management concepts and risks associated with IT or ITeS organizations
b) To expedite the existing risk analysis methodologies and assess limitations of the tools used in industry
c) To find out suitable risk analysis model based on the findings and suitability

DATA COLLECTION & DISCUSSION

Based on the industry experience, study done through relevant articles and information collected from ITeS organizations, risks associated with ITeS Organizations and analysis techniques used by them to assess and manage risks are captured. The risks faced by IT or ITeS organizations can be classified as detailed below**:**

a) RISKS ASSOCIATED WITH ITES ORGANIZATIONS

7.a.1) **BUSINESS RISKS**

i) **Governance** – without oversight, business leaders will be able to create shadow IT components or entire organizations and within IT there are fewer barriers to creating unapproved environments. It is important to understand the provider's business model to ensure they have a reasonable burn rate operating at a profit and not dependent on investment

ii) **Regulatory** – ensuring compliance with the myriad of rules including SOX (Sarbanes-Oxley Act), DPA (Data Protection Act), OHSAS (Organization Health Safety And Security), ISMS (Information Security Management Systems) and others while taking advantage of the economic model

iii) **Vendor alignment** – many vendors are researching and developing cloud products so companies may be caught unaware if a key vendor changes their business model from installed or dedicated hosting to a cloud SaaS (Software As A Service) only model.

7.a.2) **TECHNOLOGY RISKS**

i) **Staff** –Difficult to keep IT expertise as many options get open for them in the industry and want to profit from the price paid by early adopters

ii) **Infrastructure** –Network / IT Infrastructure is the most important component of any model which is highly prone for risk factors

iii) **Data** – Location of data within the network cloud may change so location restrictions must be incorporated to avoid global issues of privacy, ownership, security and discovery. When the data moves, provider must ensure old copies are securely destroyed.

iv) **Security** – securing data at rest and in transit is fundamental when using external network resources such as the internet. Once the data is secure, limiting access via identity management is critical but may require integration creating a point of vulnerability.

b) MAJOR SECURITY FLAWS OBSERVED IN COMMON & IMPACT ON IT/ITES INDUSTRIES

TABLE 2: THREATS & IMPACT

Threat-Source	**Motivation**	**Threat Actions / Impact**	
External hackers	Challenge Ego Rebellion	Hacking Social engineering	System intrusion, break-ins Unauthorized system access
Internal hackers (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	Assault on an employee Blackmail, Interception Browsing proprietary data Computer abuse, Fraud and information bribery, theft	Input of falsified, corrupted data Malicious code (e.g., virus, logic bomb, Trojan horse) Sale of personal information System bugs, sabotage
Computer criminal	Destruction of information Illegal information disclosure Unauthorized data alteration	Computer crime (e.g., cyber stalking) Spoofing	Fraudulent act (e.g., replay, impersonation, interception)
Cyber Terrorism	Blackmail Destruction Exploitation Revenge	Terrorism. Information warfare	System attack (e.g., DDoS), penetration, tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	Economic exploitation Intrusion on personal privacy, Social engineering	Unauthorized access to classified, proprietary, and/or technology-related information

c) RISK ANALYSIS TOOL WIDELY USED IN INDUSTRIES

Risk Analysis Technique is to identify, estimate, prioritize and evaluate risk of possible failures at each stage of a process.

FMEA is one of the popular tools for risk analysis widely used in many organizations. It is a proactive process used to look more carefully and systematically at vulnerable areas or processes. FMEA begins with identifying each element, assembly, or part of the process and listing the potential failure modes, potential causes, and effects of each failure. A risk priority number (RPN) is calculated for each failure mode and it is used as an index for measuring the rank importance of the items identified. FMEA can be employed before purchase and implementation of new services, processes or products to identify potential failure modes so that steps can be taken to avoid errors before they occur. In FMEA, failures are prioritized according to how serious their consequences are, how frequently they occur and how easily they can be detected. An FMEA also documents current knowledge and actions about the risks of failures for use in continuous improvement. It is used for process control, before and during ongoing operation of the process. The outcomes of an FMEA development are actions to prevent or reduce the severity or likelihood of failures, starting with the highest-priority ones. It may be used to evaluate risk management priorities for mitigating known threat vulnerabilities. FMEA helps select remedial actions that reduce cumulative impacts of life-cycle consequences (risks) from a systems failure (fault).

TABLE 3: FMEA – SAMPLE TEMPLATE

IT PROCESS: Problem/Incident/Service/Change Management									**Control plan**			**Ratings after implementation of control plan**			
Id	Activity	Failure Mode	Failure Effect	Severity	Cause	Occurrence	Detection	RPN	Description	Target	Responsibility	Severity	Occurrence	Detection	RPN
1	**Analyze the root cause of the problem**	Improper analysis	Wrong output Delayed closure; Non closure	9	Over look / Negligence	5	1	45	1. To include RCA tools as a practice 2. Train all IT engineers & familiarize on these	9 - Feb	IT Manager	5	1	5	**25**
					Lack of training	5	5	**225**							

After ranking the severity, occurrence and detectability the **Risk priority number (**RPN) can be calculated as **RPN = S × O × D** that will range between 1 and 1000. The higher the number, the greater the risk your process has at that point. High RPN items are flagged and mitigation actions initiated. Then that step can be re-evaluated allowing you to quasi-quantify the amount of risk removed from your process. In the above FMEA template, we considered **225** as threshold value for applying control plans and re-assess the RPN.

TABLE 4: CATEGORIZATION OF CRITICAL PARAMETERS: OCCURRENCE / SEVERITY / DETECTION

Rating	Occurrence - `O' (Cause of a failure mode and the number of times it occurs)	Severity - `S' (all failure modes based on the functional requirements and their effects)	Detection - `D' (Current controls that prevent failure modes from occurring)
1	No known occurrences on similar products or processes	No effect	Certain - fault will be caught on test
2	Low (relatively few failures)	Very minor (only noticed by discriminating customers)	Almost Certain
3	Moderate (occasional failures)	Minor (affects very little of the system, noticed by average customer)	
4/5/6	High (repeated failures)	Moderate (most customers are annoyed)	Low
7/8	Very high (failure is almost inevitable)	High (causes a loss of primary function; customers are dissatisfied)	Moderate
9/10		Very high and hazardous	High; Fault will be passed to customer undetected

FMEA is used extensively towards

a) Development of system requirements that minimize the likelihood of failures.
b) Methods to design and test systems to ensure that the failures have been eliminated.
c) Evaluation of customer requirements to ensure that those do not rise to potential failures.
d) Identification of certain design characteristics that contribute to failures, and minimize or eliminate those effects.
e) Tracking and managing potential risks in the design avoid recurrence of the failures.
f) Ensuring that any failure occured won't injure the customer or seriously impact system.

Limitations of FMEA: (Source: http://www.qualityportal.com)

a) The initial output of an FMEA is the prioritizing of failure modes based on their risk priority numbers. This alone does not eliminate the failure mode. Additional action that might be outside the FMEA is needed.
b) FMEA may only identify major failure modes in a system. Identifying failure modes is a team brainstorming activity. If the team forgets to list it, an important failure mode could be left alone, waiting to occur.
c) FMEA is a prioritization tool. It doesn't eliminate failure modes or effects by itself.
d) It takes time to get into the details.
e) High repeatability and reproducibility.
f) Might miss a failure mode or an effect outside the experiences of the company.
g) Customers, especially end-users and suppliers, often have a better view on failure modes than internal personnel.
h) Many FMEAs focus only on the customer requirements (specifications). Sometimes internal productivity losses, equipment damage, scrap, and rework have very severe effects on the company.
i) Templates are great but every product being made in a process is not exactly the same.
j) A control might apply to one effect of a failure mode but not another.
k) FMEA will not be a living document if it is not tied to the control plan. As new potential failure modes are identified, they should be added to the FMEA and control plans developed for them.

SUMMARY OF FINDINGS / SUITABILITY OF ANALYSIS TOOL

The existing methods are mostly based on the failure events experienced or assumed by the people involved in process execution. Even though the methods satisfy the customers to certain extent, they do not completely ensure the avoidance of failure events or extends required guidance to customers to reduce the risk factors. Hence the approach on the assets, resources involved in the system could be analyzed for a better method in risk analysis.

i) Selection of right tool for risk analysis should be based on below **needs**:

TABLE 5: NEEDS OF RISK ANALYSIS TOOL

(a) Factors/Assets affect the organization's ability to accomplish its mission or its objectives	(d) Processes where these controls installed
(b) Recent changes have been made to these processes to improve their robustness in preventing the risk having a detrimental effect on the business	(e) Measurement of effectiveness of these provisions
(c) Provisions made to contain, reduce or control risk	(f) Critical services or products are to be identified and they must be prioritized based on minimum acceptable delivery levels and the maximum period of time the service can be down before severe damage to the organization results

ii) Selected tool should **provision** to mitigate risk / provision to safeguard organization from:

TABLE 6: PROVISIONS TO BE MADE AVAILABLE IN ANALYSIS TOOL

(a) Attack by competitors, disgruntled employees, computer viruses	(g) Delayed receipt of product or payment
(b) Loosing customers, suppliers, employees, reputation	(h) Hazards injurious to health of personnel and/or the environment
(c) Decline in orders, revenue, profit, market share	(i) Accidents to personnel and equipment
(d) Dissatisfying customers, shareholders, employees	(j) Breakdown of equipment, plant, machinery, relationships
(e) Prosecution by regulators, customers, employees	(k) Business disruption by computer failure, loss of information, strikes, weather.
(f) Delayed delivery	

SOLUTION SUGGESTED / AN IMPROVED APPROACH

Through this study, we propose **Risk-Level Matrix** which can highly suit the present business environment in both IT & ITeS organizations well and the same is proved from various implementations. The detailed procedure of the approach is as below:

Step (i) IDENTIFICATION OF CRITICAL SERVICES: The ranking of critical services is measured through information gathered by observing the impact of a disruption to service delivery, loss of revenue, additional expenses and intangible losses. Key functions of ITES organizations can be categorized into 3 **groups** viz.,

TABLE 7: KEY BUSINESS PROCESSES/FUNCTIONS/DEPENDENCIES

IT Processes (Expertise)		IT Infrastructure (Equipment)		IT Services	
Network Admin	System Admin	Gateway Routers	Business Portals	Intranet connectivity	Email services
IT security support	Backend support	LAN switches	Business Laptops	Client network connectivity	IT Hardware support
IT development	Field support	Network Servers	Network Monitors	Internet connectivity	IT Applications support
IT solution architect		Firewalls & IDS	Access controllers		Alert Monitoring

Step (ii) DETERMINATION OF RATINGS FOR RISK ANALYSIS TEMPLATE

Overall risk is derived by multiplying the ratings assigned for threat **likelihood** (e.g., probability) and threat impact with the asset rank and the **Asset rank** is based on Asset value which is calculated as $\mathbf{C^2 \times I^2 \times A^2}$ (C-Confidence, I-Integrity & A-Availability).

TABLE 8: OVERALL RISK

Overall Risk (Asset Rank x Probability x Impact)			
Rank	**Category**	**Range of values**	
		From	**To**
1	Low	0	2
2	Moderate	3	8
3	High	9	36
4	Severe	37	64

TABLE 9: ASSET VALUE/RANK

Categorization – Asset Value/Rank			
Rank	**Asset Value (C*C+I*I+A*A)**	**Range of values**	
		From	**To**
1	Low	1	6
2	Moderate	7	17
3	High	18	34
4	Very High	35	48

The **impact** and **probability** is for each threat and will generally differ based on the past history and/or the expectation of the particular threat to occur in future. The thresholds for the above were defined by dividing the highest Overall risk by four and bucketing the same evenly. Such definitions are purely decided by Tactical team of organization and approved by top management

TABLE 10: CATEGORIZATION – CIA (CONFIDENCE / INTEGRITY / AVAILABILITY)

Rating	C – Confidence	I - Integrity	A - Availability
1	LOW - No impact if compromised	LOW - No impact if compromised	> 5 days
2	Medium - Some impact if compromised	Medium	1-5 Days
3	High Significant impact	High Significant impact	1 day
4	Very High / Severe / highest Impact	Very High / Severe / highest Impact	0

As mentioned earlier the rating for impact and probability are measured against each threat and vulnerability determined on the assets involved in meeting up business objectives.

Step (iii) PREPARATION OF RISK ANALYSIS TEMPLATE:

Populate the identified critical components including Expertise Resources, Equipments and Services as ASSET in below template along with their attributes like Confidence [C], Integrity [I], Availability [A]. The template helps identifying their rank and overall risk value and then the residual risk, obtained after applying the effectiveness of existing control plans. It also tracks for the proposed control plans to either nullify the risk or reduce them to the acceptable limits by top management.

TABLE 11: RISK ANALYSIS REPORT

Assets			C	I	A	Asset			Threats	Impact*	Probability ranking*	Overall Risk Value*
			Values			Value	Class	Rank				
Id	Name	Group	Confidence	Integrity	Availability	$C^2 \times I^2 \times A^2$	Very High / High / Moderate / Low	1 to 4	Identified Threats	Impact against Threat	Occurrence of Threat	Asset Rank x Impact x Probability

Overall Risk Class	Overall Risk rank	Existing Control Rating #	Existing Residual Risk	Proposed Control Rating	Proposed Residual Risk	Management decision on risk
Severe / High / Moderate / Low	0 to 4	Average of all controls Existing (0 to 4)	Overall Risk -Existing Control Rating (0 to 4)	Average of all Proposed controls	Existing Residual Risk-Proposed Control Rating	Accept / Reduce / Transfer / Avoid

*****Overall Risk Value is measured as per Table 6.2 and values for Impact and Probability is from Table 6.6:

To measure **proposed residual risk value**, existing residual risk needs to be assessed based on the existing controls against the risk factors (Average of all controls Existing). Assets with Existing Residual value of High and Very High would be mitigated to reduce the risk value to Proposed Residual Risk value less than High. The process is referred as **Risk Mitigation**.

TABLE 12: CATEGORIZATION – IMPACT / PROBABILITY / EXISTING-CONTROL

Control Rating	Impact	Probability	Existing Control
0	no impact	Unlikely to occur	no effective control
1	low	Possible to occur- 2-3 times in every 5 years	basic control -less effective
2	moderate	Possible to occur - once every year	Standard control -covers but not all
3	high	Highly Probable every month	comprehensive
4	Very High /severe	Certain every week	complete control

Step (iv) CONCLUSION & ACCEPTANCE FROM MANAGEMENT: Proposed residual risk value shall be discussed with Top management and conclude for either **acceptance** or further **reduction** of risk value or **transfer** the risk or **avoidance**. As this would impact business relation, concurrence from client organizations is sought during business agreements.

TABLE 13: RESIDUAL RISK CALCULATIONS

Existing Residual Risk	Overall Risk - Existing Control Rating
Proposed Control Rating	Average of all Proposed controls
Proposed Residual Risk	Existing Residual Risk - Proposed Control Rating

The risk remaining after the implementation of new or enhanced controls is the residual risk. Practically no IT system is risk free, and not all implemented controls can eliminate the risk they are intended to address or reduce the risk level to zero or to the acceptable level agreed by senior management. This concludes the best analysis of risk pertaining to IT or ITeS systems and the tool has been tested for acceptability and adoption.

ADVANTAGES OF USING RISK-LEVEL MATRIX

1. The approach is not based on the risk priority numbers and hence the actions required outside this tool are very minimal.
2. As the tool is meant for all critical services, need to wait for failures to occur.
3. It takes less time to get into the details.
4. Rating scales are very specific and easily understandable by both employees and Management.
5. The processes are broken into easily manageable tasks.
6. "Identification of critical services" Includes all stakeholders to ensure a better view on failure modes. No dedicated team and time to be spared for using this tool and no superficial look is required as the analysis is on the on-going services.
7. Apart from the customer requirements (specifications), this tool considers internal productivity losses, equipment damage.
8. Teams often have root causes as failure modes. A failure mode is the failure to perform the intended function.
9. Templates are simple and direct. Controls are as perceived.
10. A control might apply to one effect of a failure mode but not to another. For example, final inspection is a control against a defect impacting a customer, but it may not be a control against rework or scrap.
11. It eliminates failure modes or effects by itself.
12. The control plan tells people how to react when a failure mode occurs. New potential failure modes are identified and they are added to the control plans developed for them.

TARGET AUDIENCE

This study provides a common foundation for experienced and inexperienced, technical, and non-technical personnel who support or use the risk management process for their IT systems. These personnel include

a) Senior management, who make decisions about the IT security budget.	h) Business or functional managers, who are responsible for the IT procurement process
b) CIO/CTO, who ensure the implementation of risk management	i) Technical support personnel (Network, System, Application, Database administrators; Data security analysts), who manage and administer security for IT systems
c) The Designated Approving Authority, who decides to allow operation of IT system	j) IT system and application programmers, who develop and maintain code that could affect system and data integrity
d) The IT security manager, who implements the security program	k) IT quality assurance personnel, who test and ensure the integrity of IT systems and data
e) Information system security officers (ISSO), who are responsible for IT security	l) Information system auditors, who audit IT systems
f) IT system owners of system software and/or hardware used to support IT functions.	m) IT consultants, who support clients in risk management.
g) Information owners of data stored, processed, and transmitted	

CONCLUSION

Risk management provides a logical and systematic means of identifying and controlling risk. It is not a complex process, but does require individuals to support and implement the basic principles on a continuing basis. Risk management offers individuals and organizations a powerful tool for increasing effectiveness and reducing accidents. Since risk analysis is an important process of risk management, the tool meant for risk analysis should be flawless and effective. Also the process should be accessible and usable by everyone in every conceivable setting or scenario. It should ensure that all business managers will have a voice in the critical decisions that determine success or failure in all our operations and activities. Properly implemented, the discussed tool will always enhance performance. India has become one of the most attractive destinations for key players across the globe for indirect investment, FDI (Foreign Direct Investment), new ventures etc with economy rising at a rate higher than 9%. Export increasing year on year basis with increase in clientele base across the globe for products, services and supports. The participation with the global players has not only helped to bring the global technology, standards and practices to India but the Indian Standards of practices has improved up to international standard. The risk management practices in the subcontinent leading towards better safer and less hazardous working places in the Indian Industries.

ACKNOWLEDGEMENTS

I am highly indebted to Mr.T.V. Chalapathi Rao, my mentor for inducing me with great knowledge on this subject of operations risk management and interest created within me to develop such articles. I would like to express my gratitude towards my wife & kids for their kind co-operation and encouragement which helped me in completion of this project. I also would like to express my special thanks to industry persons for giving me their attention and time.

REFERENCES

1. Anadi Kishore Sethi, "The Indian Trends in Risk Management Practices"
2. Dale H. Besterfield, "Total Quality Management" – 3rd Edition, Prentice Hall
3. FAA System Safety Handbook: "Operational Risk Management"
4. Gary Stoneburner, Alice Goguen, and Alexis Feringa, "Recommendations of the National Institute of Standards and Technology (NIST)" Publication 800-30
5. P.K. Marhavilas and D.E. Koulouriotis, "Risk assessment techniques in work sites" Democritus University of Thrace, Xanthi, Greece
6. Resource engineering, Inc, Quality Training Portal, viewed on November 6, 2013 http://www.qualityportal.com
7. Richard B Chase, F Robert Jacobs, Nicholas J Aquilano, Nitin K Agarwal, "Operations Management for competitive advantage", Tata McGraw Hill
8. Risk PRO, India, Web Portal for professional updates, viewed on October 10,2013 http://www.casansaar.com

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Commerce, IT & Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you tosupply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mail**infoijrcm@gmail.com** for further improvements in the interest of research.

If youhave any queries please feel free to contact us on our E-mail infoijrcm@gmail.com.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-
Co-ordinator

DISCLAIMER

The information and opinions presented in the Journal reflect the views of the authors and not of the Journal or its Editorial Board or the Publishers/Editors. Publication does not constitute endorsement by the journal. Neither the Journal nor its publishers/Editors/Editorial Board nor anyone else involved in creating, producing or delivering the journal or the materials contained therein, assumes any liability or responsibility for the accuracy, completeness, or usefulness of any information provided in the journal, nor shall they be liable for any direct, indirect, incidental, special, consequential or punitive damages arising out of the use of information/material contained in the journal. The journal, nor its publishers/Editors/ Editorial Board, nor any other party involved in the preparation of material contained in the journal represents or warrants that the information contained herein is in every respect accurate or complete, and they are not responsible for any errors or omissions or for the results obtained from the use of such material. Readers are encouraged to confirm the information contained herein with other sources. The responsibility of the contents and the opinions expressed in this journal is exclusively of the author (s) concerned.

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals