Scholastic Seed Inc.

www.gjeis.com

global Journal of ENTERPRISE INFORMATION SYSTEM

Enterprise Risk Management in it and its Governance: A Pragmatic Analysis for Operational Efficiency in Banking

– V Gajapathy*

Professor, School of Management, Presidency University, Bengaluru, India, vgajapathy@presidencyuniversity.in

– K Balanagarajan

Assistant Professor, School of Management, Presidency University, Bangaluru, India, balanagarajan@presidencyuniversity.in

ARTICLE HISTORY

Paper Nomenclature: Empirical Research Paper (ERP)

Paper Code (DOI): 22806

Originality Test Ratio: 2%

Submission Online: 26-Nov-2018

Manuscript Acknowledged: 30-Nov-2018

Originality Check: 03-Dec-2018

Peer Reviewers Comment: 22-Dec-2018

Blind Reviewers Remarks: 05-Jan-2019

Author Revert: 05-Jan-2019

Camera-Ready-Copy: 15-March-2019

Editorial Board Citation: 31-Mar-2019

Published Online First: 01-June-2019

EDITORIAL BOARD EXCERPT Initially at the Time of Submission (ToS) submitted paper had a 36% plagiarism and after rectification it was reduced to 02%, which is an accepted percentage for publication. The editorial board is of an observation that paper had a successive close watch by the blind reviewer's which at a later stages had been rectified and amended by an authors (Gajapathy & balanagaraja) in various phases as and when required to do so. The reviewer's had in a preliminary stages remark with minor revision with a following statement which at a short span restructured by the authors. The comments related to this manuscript are tremendously noticeable related to **Enterprise Risk Management in it and its Governance** both subject-wise and research wise by the reviewers during evaluation and further at blind review process too. The authors have crafted the paper in a structured manner. The introduction gives a clearer perspective on the conceptual foundations about integrated risk management and governance in IT in banking operations without compromising the operational efficiency. The need is to have more in-depth analysis on the topic in the current scenario. Empirical investigation would have been added to authenticate the secondary literature. Overall the paper promises to open newer facets of studies. All the comments had been shared at a variety of dates by the authors' in due course of time and same had been integrated by the author in calculation. By and large all the editorial and reviewer's comments had been incorporated in paper at the end and further the manuscript had been earmarked and decided under **"Empirical Research Paper"** category as its highlights and emphasize the work in relation to Enterprise Risk Management in it and its Governance: A pragmatic Analysis for Operational Efficiency in Banking

ABSTRACT Operational efficiency is the most vulnerable in banking sector. A laxed operational management impairs the efficiency and finally it impacts the belief of the Indian economy as it is banking economy often. In this paper a discussion is mooted and analysis is laid upon various processes in relation to IT risk and risk management strategies available therein. This Paper also promptssome current practices which are envisaged in banking sector. A work on the tools for building operational efficiency in the course of Continuous Process Improvement (CPI) in banks is laid down. IT governance and Service Level Management process is accounted in detail. Further, Incident Management Overview process and Capacity Management Process have also been depicted. Hence, this discussion paper in IT Risk Management (ITRM) and its governance in banking delivers a launchpad-provision to the pertinent researchers. In later part of the paper, available and supported risk mitigation strategies are also discussed widely.

KEYWORDS Efficiency | Capacity | SCM | Governance | Risk Management

***Corresponding Author**

https://doi.org/10.18311/gjeis/2018.22806

Volume-10 | Issue-3 | July-Sep, 2018 | Online ISSN : 0975-1432 | Print ISSN : 0975-153X

Frequency : Quarterly, Published Since : 2009

Introduction

The non-dependence on the IT by banks is almost zero. Therefore, the zero intolerance over loss due to operational risk is in exercisealmost in all banks. There are two perspectives that may require immediate attention. First, the risk management process is anconstantly continuous iterative method. It must be repetitive infinitely. The business environment is constantly and swiftly dynamic and fresh pressures and vulnerabilities emerge every day. Next is, the choice of counter-measuresused to manage risks must strike a balance between productivity, cost, effectiveness of the counter-measure, and the value of the information-asset being protected.

Risk management is the process that permits IT practitioners to poise the operational and economic costs of protective actions and achieve gains in mission capability by protecting the IT systems and data that provision their organizations' missions. This process is not exceptional to the IT environment; indeed it permeates decision-making in all areas of our daily lives.

The head of an organizational unit must ensure that the organization has the capabilities needed to accomplish its mission. These mission owners must regulate the security capabilities that their IT systems must have to afford the desired level of mission support in the face of real world threats. Most firms have narrow budgets for IT security; therefore, IT security expenditure must be studied as thoroughly as other managerial decisions. A well-structured risk management methodology, when used effectively, can help management recognizesuitable controls for providing the mission-essential security competences.Risk management in the IT ecosphere is quite a compound, multi faced activity, with a lot of relations with other intricate activities.

Review of Literature

Risk management refers to the logical development and execution of a plan to deal with potential losses (Mark S.Dorfman, 2007). 'IT risk is the potential for an unplanned event involving a failure or misuse of IT to threaten an enterprise objective – and it is no longer confined to a company's IT department or data center. An IT risk incident has the potential to produce substantial business consequences that touch a wide range of stakeholders. In short, IT risk matters – now more than ever' (George Westerman & Richard Hunter, 2007). ITRM is the solicitation of risk management methods to Information technology in order to manage IT risk, i.e.:The assumed business risk and associated when the organization involved in the use, ownership, operation, involvement, influence and adoption of IT at an enterprise-wide level. Hence, ITRM shall also be considered from the ERM point of view. Enterprise Risk Management (ERM) is a strategic business discipline that supports the achievement of an organisation's objectives by addressing the full spectrum of its risks and managing the combined impact of those risks as interrelated risk portfolio (Paul Hopkin,

Objectives

This study predominantly captures conceptual foundations about integrated risk management and governance in IT in banking operations without compromising the operational efficiency.

Methodology

Discussion on various concepts in risk management and ERM oriented towards optimization of associated risks in operational efficiency in banks is embarked. Various pertinent processes are depicted in diagrams.

2014) (p. 207).The Certified Information Systems Auditor Review Manual 2006 produced by ISACA, an international professional association fixated on IT Governance, delivers the following description of risk management: "*Risk management* is the process of identifying vulnerabilities and threats to the information resources used by a firm in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization. ITRM along with other types of risk shall be subsumed into ERM system. 'The risk governance process is the force that pulls otherwise fragmented, localize views of IT risk together into a comprehensive whole, allowing the enterprise to effectively set priorities and act… Most large enterprises lead their IT risk management with an effective risk governance process. For all enterprises, it is essential to be competent at this discipline as rapidly as possible' (George Westerman & Richard Hunter, 2007).

The establishment, maintenance and continuous apprise of an Information Security and Management System (ISMS) provide a stout indication that the IT management is using a systematic and scientific approach for the identification, assessment and management of information security risks.Different methodologies have been proposed to manage IT risks, each of them divided in processes and steps. According to ITRM, it incorporates not just only the negative impact of operations and service delivery which can bring annihilation or decrease of the value of the organization, but also the benefit/value enabling risk associated to missing opportunities to use technology to enable or enhance business or the IT project management for aspects like overspending or late delivery with adverse business effect.

As risk is strictly tied to uncertainty, Decision theory should be applied to manage risk as a science, i.e. rationally making choices under uncertainty. The contrast between risk and uncertainty is the application of 'likelihoodness'. How far the human expectations have been mixed with the future aberrations and the computations have been fine-grained for conceptions, to determine the degree of uncertainty in a decision and to optimize it, are the matter of bettering the quality of life. "All decision makers are equally likely to profit as well as to lose; luck is the sole determinant of success or failure. Uncertainty exists when the outcomes of managerial decisions cannot be predicted with absolute accuracy, but all probabilities and their associated probabilities are known. Under conditions of uncertainty, informed managerial decisions are possible. Experience, insight and prudence allow investment managers to devise strategies for minimizing the chance of failing to meet business objectives" (Hirschey, 2009). Management of uncertainty is being widely conducted by tools such as Laplace Criterion, Savage Criterion etc. (Tapiero, 2004)

Generally, the terms risk and uncertainty have been used interchangeably. However, risk refers to uncertainty in which the possible outcomes are either 'loss or no loss' rather than with uncertainties that also present the opportunity for profit (Trieschmann, Hoyt, & Sommer, 2007). In general terms, risk is the outcome of likelihood times impact.The degree of an IT risk can be determined as a result of threat, vulnerability and asset values:

Analysis and Discussion

A bank's operating model defines the delivery mechanism to accomplish its business goals. It comprises products and services, staff systems, policies and procedures. There is a cost and risk in delivering products and services to the markets. The efficiency and maturity of the operating model determines the bank's ability to create value for its customers at optimized cosgt and minimal risk.

A new bank creates its model from scratch. It could draw from the experience of similar banks. The model for an existing bank evolves over a period and the residual risks in banking processes determines the maturity of the model

- Good operating model
- Provides the correct environment for attaining goals
- Establishes ownership for processes and/or activities
- Aligns technical processes with business processes
- Assigns and integrates systems and staff for the execution of policy procedures
- Standardizes the delivery processes and accommodates approved variations necessitated by local business conditions
- Is scalable to meet organization's growth targets
- Has the right mix of preventive and detective controls
- Allows for cost optimization and risk mitigation.

Model Optimisation

Risk and Control monitoring occurs in dynamic business setting. An Optimised Model shall be attained if the bank's obligation to CPI (Continuous Process Improvement) is sufficient. The projections and consequences pronounced in the forthcoming portion of this Paper on Tool for constructing a process-based Mature Operating model protrudes an inroad to luster the approaches to Operating Model Optimisation.

Tools for constructing Operating Efficiency

By employing the following tools the functional as well as technical processes can fully be amplified to alleviate costs in consonant withmitigating operational risks for optimising benefits:

i. Business Process Management Suite (BPMS)

ii. Information Technology Governance (ITG)

iii. Advanced Analytics (AA)

Whilst Business Process Management Suite and IT Governance help model and compose process based banking activities, Analytics allows and paves a way for the Operations Group and other functions, to monitor the performance and continuously headway the processes.Of the above, ITG shall be discussed as follows:

Information Technology Governance (ITG):

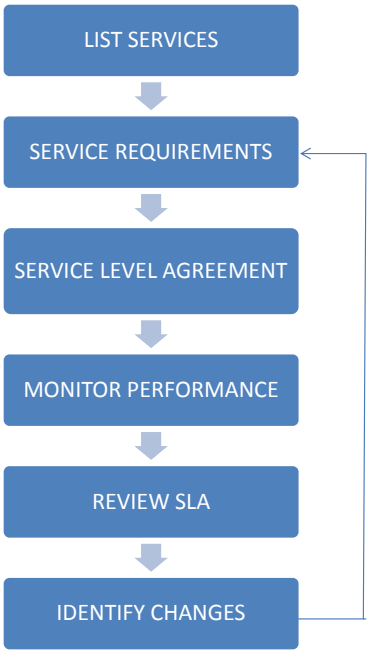
In normal course of action, the governance model shall allow the evaluation of technology usage for the purpose of improving business processes and line up technology in response to the business. The model also takes care of resource deployment on priority front. Employ Business Impact Analysis (BIA) to set priorities and timelines for the purpose of recovery. 'BIA takes senior management's discussion of tolerance for availability risk to a detailed level, including assessment of how failure in specific business processes will affect the business over time, hour by hour and day by day, and the circumstances in which processes might fall' (George Westerman & Richard Hunter, 2007).

ITG predominantly has two components inherently, as follows:

- Governing Knowledge consists of Objectives, Policies, Strategy, Scientific Procedures and Superior Practices. Each part has greater import in its importance for the IT Governance and its practice.
- IT Governance Tool.

Service Level Management

Management includes both internal and external Service Level Agreements. It includes Vendor Management.Process-1: Service Level Management.



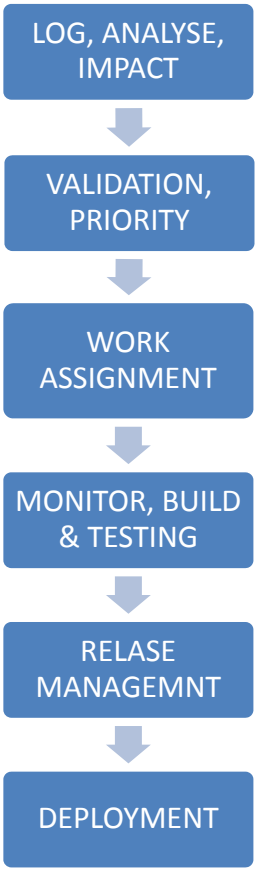
Availability Management

This is the overall architecture of the organization. It would include theclients, messaging, routers, bridges, servers, operating systems, system software, load balancing, firewalls, bandwidth and internet management.

Incident Management System

IMS of anorganization would usually includeintrusions, incidents and the response system. The objectives are (i) Roles, responsibilities and Training (ii) suitable tools are accessible for the purpose, (iii) Protection of assets

Process-2 – An Overview of an Incident Management



Application Management

The entire spectrum of an organisation's solution architecture could be classified into Non-production and Production systems. Commonly a higher severity is the concern entwined with the Production Environment.

Change Management

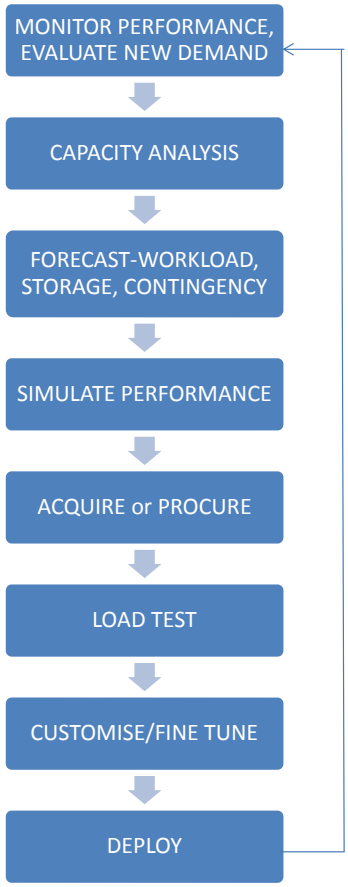
Identifying a change is the challenge for the governance model. Once, it is identified, then eventually the authorization process will also be solidified.

Asset Protection subsume Source Code Management in its fold. Additionally, Along with software vendors, Escrow Agreements should also be in place.

Management of Capacity

Figures with respect to Business growth are ingredients for theprospectiveexercise. Depending on the expectedgrowth, the infrastructure team confirms the risks of having capacity constraints if service support and delivery are minimalized.Every ITIL element is process oriented. The following figure is, for instance, providing an overview of Management of Capacity.

Process-3: Management of Capacity



The processes exhibited *supra* are beneficial in ITRM (ITRM) and its governance.For the continuity of banking business, Riskmitigation strategies are decisive and most imperative amongst.

Risk Mitigation:

Risk mitigation as a part of the ERM is an application of methodical approach by senior management to appease mission risk. Specialists need to understand lots of details, but most people only need to understand risk in terms of what create risk for them and what they can do to reduce their vulnerability to those risks (George Westerman & Richard Hunter, 2007). The following risk mitigation alternatives are available:

- **Risk Assumption**. Assuming the potential risk and harvesting the benefits of operating the IT system or to exercise controls to reduce risk at a desired state.

- **Risk Avoidance**. If the peril or source of the risk is avoided, the exposure itself shall be minimized.

- **Risk Limitation**. A good management control system limit the quantum and frequency of risk exposure.

- **Risk Planning**. To develop a risk mitigation plan which is destined (to manage risk) to prioritize, implement, and maintain controls

- **Research and Acknowledgement**. Identifying or acknowledging vulnerability, which increases exposure, involves research. This vulnerability leads to risk and consequently chance to loss or loss itself are result. In order to implement control, research should be in place to correct vulnerability.

- **Risk Transference**. Insurance planning holds high importance both for cost consideration and risk transfer. Apart from insurance, other methods may be explored for transference.

Report the greatest risks and work for sufficient risk reduction at the lowest cost, with minimal impact on other mission capabilities.The term methodology means an organized set of principles and rules that drive action in a particular field of knowledge. A methodology does not describe specific methods; nevertheless it does specify several processes that need to be followed. These processes constitute a generic framework. They may be broken down in sub-processes, they may be combined, or their sequence may change. However, any risk management exercise must carry out these processes in one form or another. The following table compare the processes foreseen by three leading standards. ISACA Risk IT framework is more recent. The Risk IT Practitioner-Guild compares Risk IT and ISO 27005. The overall comparison is illustrated in the following table.

With respect to the probabilistic nature and the requirement of cost benefit analysis, the process in the management of IT risk, in the lines of NIST SP 800-30, can be divided in the following processualsteps.

Effective risk management is of the characteristic of complete assimilation into the Systems Development Life Cycle. The analysis of Information risk conducted on applications, computer installations, networks and systems under development should be administered using structured methodologies.

Finally, operationalizing a strategy for ITRM means incorporating it into the enterprise's foundation, observing risk governance process, and conducting risk awareness programs (George Westerman & Richard Hunter, 2007).

Risk management constituent processes

CONTEXT			Risk IT
Context establishment	Organizational context		RG and RE Domains more precisely • RG1.2 Propose IT risk tolerance, • RG2.1 Establish and maintain accountability for ITRM • RG2.3 Adapt IT risk practices to enterprise risk practices, • RG2.4 Provide adequate resources for ITRM, • RE2.1 Define IT risk analysis scope.
Risk assessment	Risk assessment	Risk assessment	RE2 process includes: • RE2.1 Define IT risk analysis scope. • RE2.2 Estimate IT risk. • RE2.3 Identify risk response options. • RE2.4 Perform a peer review of IT risk analysis. In general, the elements as described in the ISO 27005 process are all included in Risk IT; however, some are structured and named differently.
Risk Awareness	Risk-Aware Culture	Risk Information	Affected employees must informed of new risk priorities and the rationale behind them, and managers at all levels must show support in word and deed.
Risk treatment	Risk treatment and management decision making	Risk mitigation	• RE 2.3 Identify risk response options • RR2.3 Respond to discovered risk exposure and opportunity
Risk acceptance			RG3.4 Accept IT risk
Risk communication	Ongoing risk management activities		• RG1.5 Promote IT risk-aware culture • RG1.6 Encourage effective communication of IT risk • RE3.6 Develop IT risk indicators.
Risk monitoring and review		Evaluation and assessment	• RG2 Integrate with ERM. • RE2.4 Perform a peer review of IT risk analysis. • RG2.5 Provide independent assurance over ITRM

References

1. **Hirschey, Mark**. *Managerial Economics-An Integrative Approach*. New Delhi: Cengage Learning, 2009.
2. **Paul Hopkin.***Fundamentals of Risk Management - Understanding, evaluating and implementing effective risk management*. 3rd. New Delhi: Kogan Page Limited, 2014.
3. **Tapiero, C**. *Risk and Financial Management: Mathematical Computational Methods*. New York: John Wiley & Sons Limited, 2004.
4. **Trieschmann, James S., Robert E. Hoyt and David W. Sommer**. *Risk Management and Insurance*. 12. Thomson South-Western, 2007.

GJEIS Prevent Plagiarism in Publication
The Editorial Board had used the ithenticate plagiarism [http://www.ithenticate.com] tool to check the originality and further affixed the similarity index which is 2% in this case (See Annexure-I). Thus the reviewers and editors are of view to find it suitable to publish in this Volume-10, Issue-3, July-Sep, 2018

Annexure 1

ENTERPRISE RISK MANAGEMENT IN IT AND ITS GOVERNANCE: A PRAGMATIC ANALYSIS FOR OPERATIONAL EFFICIENCY IN BANKING

ORIGINALITY REPORT

2%	0%	0%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

MATCH ALL SOURCES (ONLY SELECTED SOURCE PRINTED)

1%
★ Submitted to Kennesaw State University
Student Paper

Citation
V Gajapathy and K Balanagarajan "Enterprise Risk Management in it and its Governance:A pragmatic Analysis for Operational Efficiency in Banking", Global Journal of Enterprise Information System. Volume-10, Issue-3, July-Sep, 2018. (www.gjeis.com)

https://doi.org/10.18311/gjeis/2018.22806
Volume-10, Issue-3, July-Sep, 2018
Online ISSN : 0975-1432, Print ISSN : 0975-153X
Frequency : Quarterly, Published Since : 2009

Google Citations: Since 2009
H-Index = 96
i10-Index: 964

Source: https://scholar.google.co.in/citations?user=S47TtNkAAAAJ&hl=en

Scholastic Seed Inc.

Conflict of Interest: Author of a Paper had no conflict neither financially nor academically.