M-RiCM Risk Analytic Model – The Case of a Telecom Company

Praveena K R[1], MCom, ACA, CISA

Murali R S[2], FCA, ACMA, CMC, CISA, CRISC, PhD

Abstract

As a result of constant changes in the macro and operational environments, organisations are exposed to fascinating combinations of risks that are dynamic. Organisations have been trying to develop various strategies to handle such dynamic risk conditions. Comprehensive approaches to understanding and managing risks through modelling multiple variables and their behaviour are also evolving.

This paper discusses an analytic model called M-RiCM that has been developed and implemented in one of the SAARC countries in the telecom sector. The paper seeks to discuss methodologies for profiling of risks and managing them. This directly influences the top management's strategic decision-making for improved quality of corporate governance, reducing the risks that the corporates are facing increasingly. The model is appropriate for organisations that face big data environment with huge number of variables and ever changing external/internal issues to handle.

M-RiCM provides quantitative score in five areas: Strategic, Operational, Financial, Compliance, and Data. The model also provides a Risk-Control Radar and an overall Risk Score, profiling each type of risk based on field level operations data across all the functions. This model is expected to substantially reduce the burden in identifying risks, documenting them, profiling them, and assigning quantitative score, and indicate ways of handling them. The model would dove-tail perfectly with current trends of industry that is moving towards technology upgradation like robotics.

The model can be linked to ERP (enterprises resource planning), CRM (customer relationship management), RPA (robotics process automation), VRI (virtual reality interfaces). The paper

[1] Praveena KR is Senior Consultant at MaGC Private Limited (praveena@magc.in)

[2] Murali RS is Principal Consultant & Managing Director at MaGC Private Limited (muralirs@magc.in)

provides detailed insights taking the case of telecom sector. The model, however, is generic and can be applied to any sector and size of organisations. The paper concludes by giving insights into practical issues and implementation challenges. It discusses recommendations and provides inputs for future research.

Key Words

Risk Analysis, Risk-Control scoring model, Control scoring, Risk-Control Radar, Corporate Governance

---

M-RiCM Risk Analytic Model – The Case of a Telecom Company

1 Introduction

Risks are ubiquitous. With fast track changes taking place in the market place, technology space, and governance; risk management has become a strategic consideration. Sustainability of organizations depend on the effectiveness of the risk management.

According to the International Federation of Accountants (IFAC), “Organizations face a wide range of uncertain internal and external factors that may affect achievement of their objectives—whether they are strategic, operational, or financial. The effect of this uncertainty on their objectives can be a positive risk (opportunities) or a negative risk (threats). Risk management focuses on identifying threats and opportunities, while internal control helps counter threats and take advantage of opportunities”. (IFAC, 2018).

Risk management has historically been related only to fixed assets. In recent times, the definition of assets has become more inclusive and today assets include rights, intellectual property, patents, knowledge, data, and so on. Organizational systems and processes are also assets, which are exposed to risks and need to be managed.

The focus of business houses and organizations across sectors is not just on their operations and profitability, but also on addressing the risks they face. “The change in emphasis from simplistic "profit-oriented" management to risk/return management can also be seen in non-bank corporations. Many major corporations are now engaged in active risk management” (Crouhy M, 2004). From a process perspective, irrespective of the type of risk, higher the control, lower the probability of risk occurring. “Risk management is the process of identifying, assessing and controlling threats to an organization's capital and earnings. These threats, or risks, could stem from a wide variety of sources, including financial uncertainty, legal liabilities, **strategic**

management errors[3], accidents and natural disasters" (Web-search, 2018). Risk management is no more confined to the top few or the board of directors. While persons responsible for governance would still need to initiate risk management activities, risk management per se is distributed across the organization and is eventually part of organizational culture. The paper is the result of organizational research in order to link risk management perspectives to both strategic and operational management.

Internal control systems have always been the major tool for risk management. This paper develops an implementable and simple model called M-RiCM for addressing risk. M-RiCM is expected to make the risk management process more objective and scientific; and support the internal processes and control mechanisms.

This paper is presented in following parts:

Part 2 – Understanding the need for the Model – issues facing industry

Part 3 – Objectives of this paper

Part 4 – Analysis of various approaches and risk analysis models

Part 5 – The M-RiCM Model

Part 6 – M-RiCM implementation - The case of Telecom Company

Part 7 – Summary & Scope for further study

[3] Highlight by the authors

2 Understanding the need for the Model – issues facing industry

Understanding risks

"Risk is the potential of gaining or losing something of value….. Risk can also be defined as the intentional interaction with uncertainty. Uncertainty is a potential, unpredictable, and uncontrollable outcome; risk is a consequence of action taken in spite of uncertainty" (Wikipedia, 2018). The losing something of value in the business or organizational context would mean losing market share, revenue, and ultimately scope for existence. Organizations perennially strive hard to prevent risks and to protect themselves from the manifestations of the same. This implies risk management. "Risk management is the art of using lessons from the past in order to mitigate misfortune and exploit future opportunities…—in other words, the art of avoiding the stupid mistakes of yesterday while recognizing that nature can always create new ways for things to go wrong" (Coleman, 2011). The risk management should hence consider the experience of the organization in addressing risks.

Another important element to risk management is what lies ahead - the probable changes in the environment – the futuristic considerations. "The risk-management process involves identifying exposures to potential losses, measuring these exposures, and deciding how to protect the company from harm given the nature of the risks and the company's goals and resources" (Reference for Business - Risk Management, 2018). The term 'potential losses' signify the futuristic considerations that organizations need to take in order to have an effective risk management system. Recently, in the Harvard Business Review, Rice and Zegart (Rice C, 2018) identified three aspects of risk that will influence in the 21st century: politics, supply chain, and technology. M-RiCM seeks to address the supply chain and technology aspects.

These discussions highlight that any risk management system should take into consideration the past, the likely future, and address supply chain (processes) and technology.

Understanding the risk management needs of industry

Irrespective of the industry, an organization faces risk. These risks are classified in several ways in order to understand and manage them. IFAC classifies risks into: strategic, operational, financial (IFAC, 2018). Risks are generally classified per industry. Insurance industry classifies risk as: market, credit, insurance and demographic, operational, liquidity, strategy, frictional, and aggregation and diversification (P.O.J.Kelliher, 2011). Top risks in the Technology industry include regulations, data security/privacy, competition, economic conditions, international operations, and so on (BDO, 2017) . (Juneja) lists credit, market, operational, moral hazard, liquidity, reputational lists as major risks in banking industry; amongst others. Key risks in the Telecom Industry are compliance/regulatory, operational, strategic, data & cyber security, and financial (E&Y, 2014) & (BDO, 2015). Hence, the risk perceived by each industry may be different, but they all relate to both internal and external factors. All these risks need internal systems (called internal controls) to identify and address them properly. Thus, risk management needs of organizations lead to robust internal control mechanisms.

Need for a comprehensive model and its role

Where do risks occur? Risks arise in processes. Irrespective of the nature of risks, risks arise when some aspects of organizational processes have not been addressed properly. Risks arise from both external and internal sources; however, unless the internal systems for identifying and handling risk is robust, organizations tend to fail. Gaps in processes resulting in risk could be in any strategic or operational processes giving rise to strategic or operational risks. The common rationale behind all risk classifications is to manage the risks for reduction of their impact on the performance of the organization and achieve organizational objectives. Is it then possible to have a common risk management framework across industries to handle risks? Yes, and such frameworks are evolving. Increasingly, all the risks in organizations are mapped to processes and by proper alignment of process and controls the risks can be handled properly.

The use of models brings undoubted benefits, including automated and objective decision-making (Carazo J.L., 2016). Better the process controls, better the risk management. Thus, if organizational risks need to be identified and addressed, appropriate models considering various

risk sensitive parameters becomes imminent. These parameters need to consider the internal controls in organization, as internal controls address the identification and handling of risk appropriately.

Various models on internal control assessment and risk assessment (detailed in part 4), provide valuable guidance and robust framework. However, these models do not seem to adequately link business process, internal controls, and risk. A comprehensive model linking these are required from several perspectives, for instance:

- Internally – the Management requires a tool to understand where they stand with regard to risks and finetune their risk management strategy;
- Externally – compliance requirements such as Internal Financial Control (under the Indian Companies Act, 2013) require the Board to have clarity on risks and control of the same;
- Auditors – need an understanding of the risk management strategy in order to express their opinion;
- Investors – need the risk profile of the organization in order to see whether their moneys will be safe with the organization.

3 Objectives of this paper

The objective of this paper is to identify, develop, and discuss a suitable **risk analytics model** taking into consideration the requirements of the industry, organizational processes, and operational aspects.

The paper specifically focuses on **developing a model** to:

i. Assess and quantify extent of internal control objectively based on business processes,
ii. Classify and represent risks into controllable elements for enabling simplified risk management initiatives.

4 Analysis of various approaches and risk analysis models

Risk management and internal control systems

In the perspective of risk management process taken up in this paper, the responsibility for risk management needs to be understood. The ultimate responsibility for risk management lies with the Board of directors; however, the risk management system exists across all levels and functions of organisations. "In principle, there is no difference between a risk management system and an internal control system. …. the scope of each phrase seems to be getting wider, and they are converging." (Leitch, 2004).

How do organisations address risks? Organisations address risks through proper corporate governance. While there are multi-faceted ramifications for this, in summary, organisations have: a professional, performing, diversified Board, good policy framework (including risk management policy), robust processes, and effective internal control systems. These when supported by capable human resources and well deployed IT infrastructure, optimal risk management takes place. "Enterprise risk management (ERM) is applied from strategy through execution, while relying on internal control at critical junctures. The two are interconnected, but not interchangeable. Indeed, when used together, they're powerful complements in supporting management" (Dennis Chesley, n.d.).

One overriding condition for the success of the risk management system is an effective internal control system.

Internal control systems enable the implementation of the decisions of the Board, adhering properly to the policy frameworks, providing appropriate controls in processes, and so on. One of the key conclusions in this regard is that "Construction of a new internal control mechanism which is reasonable and reflects the risk management can reduce input costs when enterprises implement the internal control risk monitoring mechanism. It will control the risk within the acceptable range

effectively" (Li, 2013). Thus, the quality of the internal control systems decides the quality of risk management of an organization.

Models considered and their approaches

In developing M-RiCM, the following three important, globally accepted and implemented risk management models/frameworks were studied:

- Committee of Sponsoring Organisations of the Treadway Commission – COSO-Enterprise Risk Management (ERM) framework
- Information Systems and Control Association – ISACA - Control Objectives in Business – COBIT model
- Institute of Internal Auditors - Comprehensive Assessment Model – CAM

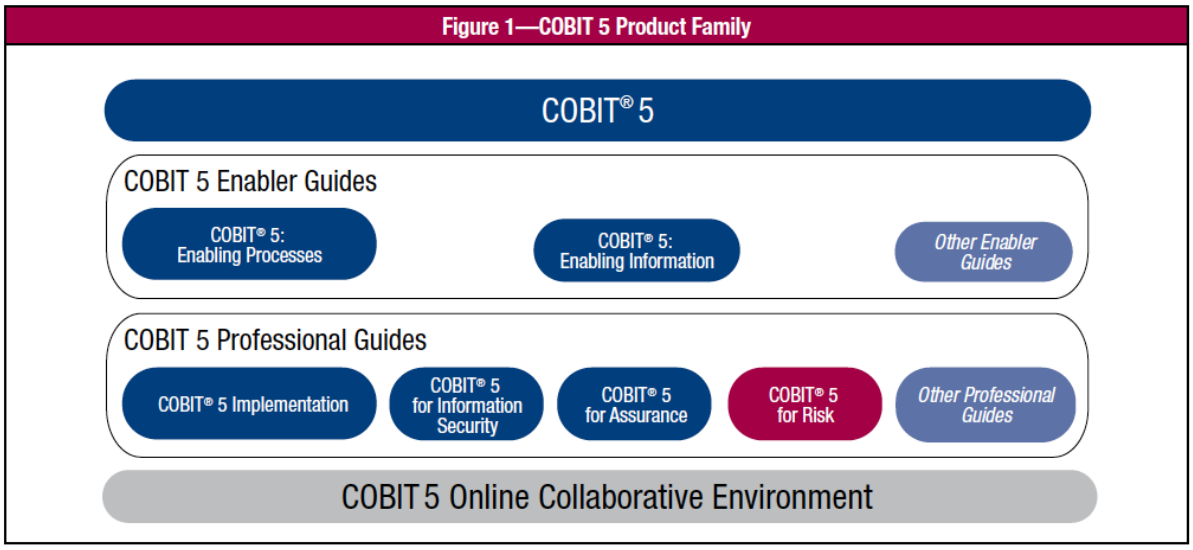
COSO- ERM

"Enterprise Risk Management—Integrating with Strategy and Performance clarifies the importance of enterprise risk management in strategic planning and embedding it throughout an organization—because risk influences and aligns strategy and performance across all departments and functions" (COSO, 2017).

This is a generic framework which provides guidance for end-to-end enterprise risk management (ERM). This framework has attempted to link strategy and implementation taking risk perspective into account.

ISACA- COBIT 5.0

COBIT 5.0 is a leading framework for governing and managing enterprise IT. It comprises of a toolkit which helps assess process controls. COBIT 5.0 (ISACA, 2013) considers the need for enabling processes. However, the COBIT is restrictive to IT process, and focuses on IT related risks.



IIA - CAM

Comprehensive Assessment Model (CAM) for ERM (IIARF, 2014) promotes full integration of entity objectives and provides a control assessment methodology. This report recognises the importance of "internal audit approach of evaluating risk management and internal control systems on a process basis…… The evaluation of the adequacy of the architecture or design of the internal control system must be conducted process by process. CAM classifies control objectives as -

strategic, compliance, operational, and financial. CAM applies principles which corroborate that - lower the control, higher the risk.

An assessment of these risk management frameworks brings out the linkages between processes controls and risk emergence. But the models have not addressed the possible specific linkages between process and controls; and how to handle them.

Taking cue from these learnings, the M-RiCM model is an attempt to link the processes to the risks.

5 The M-RiCM Model

M-RiCM[4] is MaGC's Risk-Control Matrix Model. M-RiCM contemplates objectively scoring degree of internal controls at process level and linking it to audit conclusion on Risk Management. M-RiCM envisages use of simple tools and a visual representation of Control Score and Risk.

The model groups risk into five classifications as follows:

1. **Financial risks (FR)** - Forex/currency fluctuations, Interest rate fluctuations, inability to access credit, poor liquidity and cash flow, uncontrolled costs, poor capital investment, credit/collection related, and fraud.
2. **Operational risks (OR)** - product/service failure (Example- service and network interruption in Telecom), overdependence on suppliers, not adapting operations to market changes, supplier error, unfavourable litigation, risks related to recruiting and retaining talent, customer dissatisfaction.
3. **Compliance risks (CR)** - unfavourable changes to regulation, non-compliance with applicable statutes and regulations (Example: Telecom Regulatory Authority's regulations, Companies Act, Income Tax Act).

[4] The model is called M-RiCM: M- MaGC® the name of the company which conducted the research, Ri – risk, C – control, and M – matrix.

4. **Data risks (DR)** - not maintaining data privacy, lack of cyber security, data hacking, data loss, threats to physical infrastructure.
5. **Strategic risks (SR)** - increased competition, fast arrival of new technologies, technology substitution, climate change natural disasters, changing customer preference, reputational risk, dependence on key personnel.

Businesses have inherent risks[5], which are reduced on application of effective internal controls[6]. The aim of Risk Management is to ensure that the Residual Risk (after application of internal controls on inherent risks) is within its pre-determined tolerance level/threshold (commonly referred to as Risk Appetite). Control Risk is the risk that the set internal controls are ineffective or fail[7]; it increases to Residual Risk (Figure 1). If the internal control mechanisms do not address them, they impact the organisation. So risk management is about addressing the control risks.

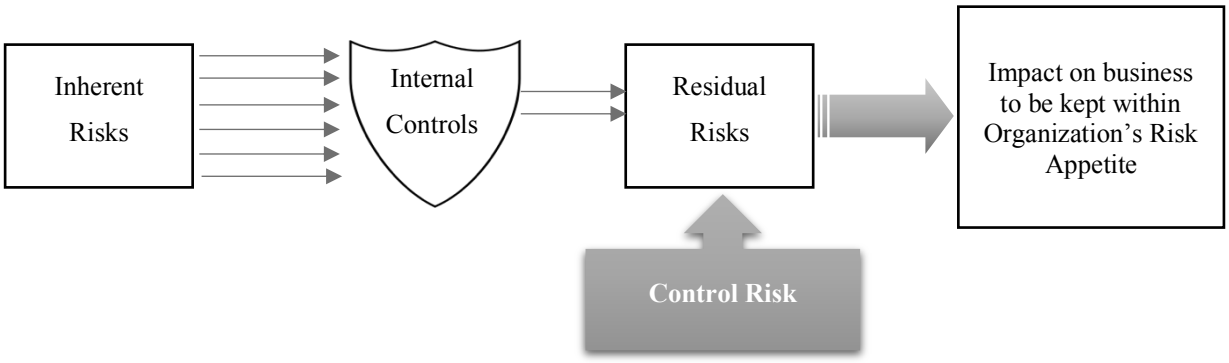


Figure 1: Risks and Controls in an Organisation

[5] ***Inherent risk*** (PCAOB) *is the susceptibility of an assertion to a material misstatement, assuming that there are no related controls.*

[6] ***Control*** (IIA-IPPF)**-** *Any action taken by management, the board and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved.*

[7] ***Control Risk*** (PCAOB) *is the risk that a material misstatement that could occur in an assertion will not be prevented or detected on a timely basis by the entity's internal control. That risk is a function of the effectiveness of the design and operation of internal control in achieving the entity's objectives relevant to preparation of the entity's financial statements. This has been defined from the perspective of financial control; however, applicable to all risks.*

M-RiCM is based on this principle expressed in Figure 1. It is designed to identify the process level controls, quantitatively evaluate the degree of control, and use it to conclude on Risk. These are achieved in three simple steps, each addressed by one component (Figure 2):

Figure 2: Components of M-RiCM

Components of M-RiCM

M-RiCM comprises of three components – Process controls inventory, Scoring Mechanism & Risk-Control Matrix, and Risk-Control Radar (Figure 3). The components have been explained below:

i. **Process controls inventory –** comprises of key business process-wise inventory of internal controls. Each internal control (process control) is linked to a Risk Classification, i.e., one that is primarily gets affected if the internal control fails. This is designed as a checklist/document which allows users to score the degree of control in respect of each line-item (internal control).

ii. **Scoring Mechanism & Risk-Control Matrix** – Control scores are determined based on evaluation of each process control (internal audit) for control existence, adequacy, and effectiveness. M-RiCM allows determination of Control Score at four levels:

   a. Each internal control scored based on audit evidence;
   b. Risk classification-wise Control Score is computed as a simple average of all internal controls pertaining to each risk class;
   c. Control Score of business process calculated as a simple average of all controls scored in the checklist (controls marked as 'Not Applicable' are eliminated);
   d. Control Score of the business unit calculated as a simple average of all its business process control scores;
   e. Overall Control Score for the organization computed as an average of business unit-wise scores. Depending on the importance attached to each of the five risk classifications, weights can be assigned to get a weighted average score, if appropriate.

   The scores at business unit /overall organization level (d & e above) are represented in the form of a Risk-Control matrix- tabulated process/business unit-wise across the five risk classifications.

iii. **Risk-Control Radar** – The principle behind the risk radar is - where internal controls are scored higher, Risk is lower, and vice versa. Applying this principle, the Control Scores are translated into an interpretation of the corresponding Risk (given in Table 1).

Table 1: Risk interpretation

Average Control Score	Risk interpretation	Remarks on scenario
Less than equal to 1.5	Very High	low control & very high risk
1.6 to 2.5	High	medium control & high risk
2.6 to 3.5	Medium	high control & medium risk
More than 3.5	Low	very high control & low risk

The average scores for the five areas (and the corresponding Risk interpretation) are diagrammatically represented as a Risk-Control Radar. Each axis in the Radar represents one of the five risk classifications. The average control score pertaining to all processes that impact the said risk classification is plotted on the axis. The five points are connected, and bounded area is shaded to represent the extent of control (pentagon as there are five risk classifications). Uncovered portion is uncovered risk.

The background in the Risk-Control Radar shows the Risk landscape (as described in Table 1 and shown in Figure 3) as four[8] concentric pentagons. The innermost pentagon representing Very High Risk (in red) and the outermost representing Low Risk (in green).

The control score representation (as shaded region) is superimposed on the Risk Landscape. This facilitates visual representation of extent of Control against Risk.

Risk-Control Radars are prepared at process level, location/business unit level, and organizational level.

[8] Number depends on the rating scale chosen

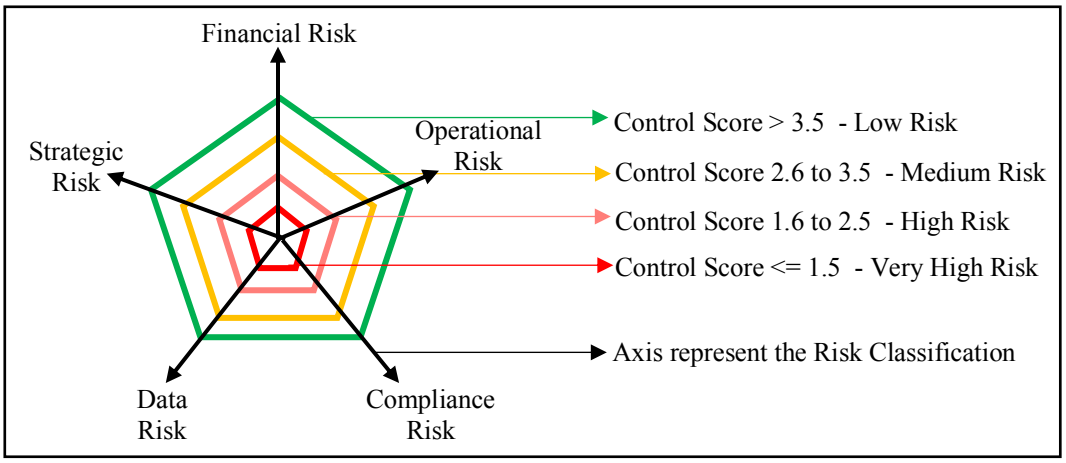


Figure 3: Risk Landscape – Scale of Risk-Control Radar

Risk-Control Radars are prepared by a function independent of Management (such as Internal Audit) and compared with the Risk Register prepared by Management. Based on the comparison, conclusions are drawn on Risk Management.

6 M-RiCM implementation - The case of Telecom Company

Approach to development and implementation

M-RiCM has already been implemented in a telecom company. The implementation involved: definition of the company's requirements, evaluation of the limitations and suitability to instant case, testing the model on three key business processes, obtaining feedback from the stakeholders on the model's robustness and applicability, and fine-tuning and finalisation of the model for implementation. The major steps were:

i. **Process Controls Inventory** - This was prepared as Audit Checklists comprising of checks for each internal control in the process and was linked to the corresponding Risk Classification impacted by its failure (Figure 4). Checklists were developed as spreadsheet

templates for 26 key business processes with about 25 process controls (average) identified in each. A sample[9] filled Audit checklist for expense process is given in Figure 4.

ii. **Scoring Mechanism & Risk-Control Matrix -** A 4-point scale[10] was applied to score controls - with 1 representing very poor control, to 4 representing very high control. Similarly, a 4 point scale was applied for risks too – Low, Medium, High, and Very High. This was fitted to match the existing Risk Register rating scale.

The process/location level scores were computed as simple average; and organization level score computed as weighted average. Weights were assigned considering revenue and expenses of each location, as only these variables found to reflect the operational volume and complexity, needed for assigning scores.

iii. **Risk-Control Radar** – These were colour coded to match the existing Risk Register rating scale.

[9] This is not the exhaustive checklist and only a sample.

[10] In the first implementation, scoring mechanism was on a scale of 1 to 4 to suit the Client's pre-existing Risk Management system. The authors recommend choosing a rating scale depending on organization's size, business, risk maturity, etc. Ideally should have odd number of points, say 5 or 7. However, care should be taken to standardize this scale if comparisons are to be drawn between organizations or on a time series.

S.no	Checks to be undertaken *T Code and report references in link below*	Risk Classification	Control Level	1	2	3	4	Coverage	Audit notes
A	**Bill Passing and expense booking**								
1	Is the name of company (xxx) reflected in the bills/invoices/supporting documents (only expenses belonging directly to BTL should be recorded)?	FR	4						
2	Are expenses recorded only based on original bill/invoice/expense statement?	FR	4						
3	Are there adequate controls to prevent processing of duplicate bills (Ex: Payments made only against original bills, automated controls, giving same bills reference twice)?	FR	3						xx out of xx instances where payments made based on photocopy of invoices
4	Are bills/invoices appropriately checked and approved before being passed on to F&A (with agreement, Purchase Order, Work Order, Goods Received Note)?	OR	3						xx out of xx instances where payments not approved by competent authority
5	In case of any entries in SAP required, are they made before being sent to F&A (Ex: GRN, project expense, payroll processing)?	FR	4						
6	Are there checks to ensure expenditures are within the budgeted amount? Are excess spends made with prior approval?	FR	3						Budegt exceeded by XX%. Approval obtained only for xx%
7	Is there a checker control to ensure expenses are recorded under the correct account head (other than automated entries)?	FR	4						
8	Is TDS accounted correctly for all applicable transactions?	CR	2						Tax not dedcuted for xx transactions out of xx (value xx%)
9	Are bills/invoices filed with respective vouchers?	OR	2						

Figure 4: Audit Checklist sample

In the sample given in Figure 5, Risk-Control Radar pertaining to Expense processes has been shown. Financial risk is best controlled – evidenced by score of 3.7 (out of 4), more shaded region, and less risk landscape exposure. However, Data Risk is where maximum risk exposure evidenced by score of 1.4 (out of 4), less shaded region, and more risk landscape exposure.

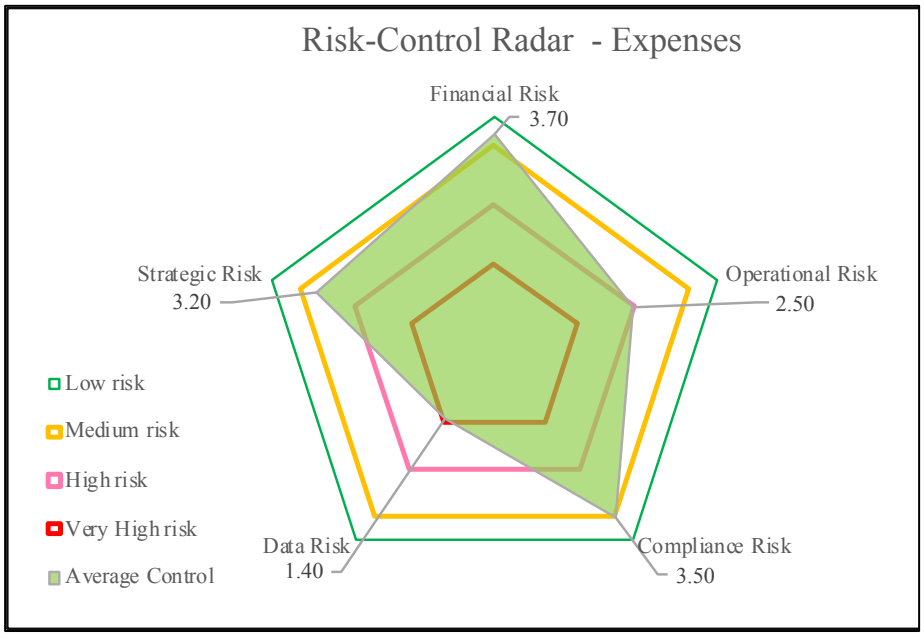


Figure 5: Risk-Control Radar sample

Risk-Control Radar is interpreted as follows:

- Greater the shaded region, higher the control; and
- If the inner pentagons (higher risk) are exposed, risk is higher.

7 Summary & Scope for further study

Currently, organizations are becoming delayered, boundaryless and focus on customer delight (both internal and external) based on robust processes and controls. Hence, the need of industry is to have a robust process control mechanism that promotes internal control and hence reduces risk. M-RiCM provides a visual representation of the Risk-Control status, considering various processes and activities under each of those processes, and hence is comprehensive.

Study objectives achieved

The objective of this paper was to develop a **risk analytics model** that would:

i. Assess and quantify extent of internal control objectively based on business processes: *The model has responded to it through its checklist addressing individual activities in processes and hence is expected to reflect all the risk areas and thus the areas requiring control.*

ii. Classify and represent risks into controllable elements for enabling simplified risk management initiatives: *The model has enabled the classification of various process into five types of risks (the case study taken up) and gives a score indicating the extent of control prevalent in the organization.*

Advantages and application

- M-RiCM model is simple and easy to understand and hence, easily implementable.

- The model is built on basic processes and activities, hence, accountability can be easily built in and monitored.

- The model is scalable and can be customized to suit organizations in different sectors and of varying sizes. Depending on the types of risks and their classification (number of axes), and the control rating scale (points in the axes odd or even) organization specific Risk-Control Radars can be prepared.
- It structures the internal audit feedback such that, if Risk Indicators are captured real time, Risk can be profiled and monitored real time too. Hence, M-RiCM has potential to be a real time control.
- Compliance with globally accepted standards such as COSO/COBIT/ISO can be embedded in the M-RiCM model.
- The model would dove-tail perfectly with current trends in technology. The model can create data on the controls dynamically and with proper IT interfaces the data can feed into ERP (enterprises resource planning), CRM (customer relationship management), RPA (robotic process automation), VRI (virtual reality interfaces). This will significantly improve the risk management and compliance abilities of organizations in the days to come.
- The model is visual and clearly expresses the extent of control available and hence very easy to interpret, for persons at different levels of the organization.
- The model is quantitative, and the final control score is just one number. This number can be monitored in time series or between divisions and organizations within a group.
- At a glance, comparisons can be made – between processes, between two business units, or between periods. Since risks are profiled at all levels, drill down from organization level to process level is feasible. Hence, processes/business units where controls are weak, and risk is high can be easily identified, corrective action initiated, and monitored.
- Using tools like LAMP® (MaGC, n.d.), the correlation between the individual risk elements can be analyzed, and exact process/activity gap that gives rise to the risk can be identified and controlled.
- The requirements of several stakeholders could be addressed with one single model. The management, the executives, departmental heads, investors, auditors, and so on can be benefitted from this model.

- Risk registers maintained by organizations will be fully supported by the process level linkages by enabling this model. With proper IT interventions, the risk registers be can be automated and the variance report on the risks can be automatically generated.

Challenges

Challenges while implementing M-RiCM include:

- Certain process controls may link to multiple Risk classifications – The model in its current form assumes that each process control is mapped to one risk classification (primarily impacted). However, practically more than one may be impacted.

- Initial difficulty in correlating Risk Classifications (as per M-RiCM) to Risk Register – This is an initial orientation issue, as Governing Body, Management, and Internal Audit need to understand and classify business risks in similar manner. This can be overcome by holding joint risk assessment/profiling by all stakeholders.

- Risks not controlled by organization's internal controls may get missed out – M-RiCM primarily evaluates Control Risk. Hence, other contributors to Residual Risk which are not subject to process controls are excluded from the scores/Risk-Control Radars.

Scope for further study

M-RiCM model can be used to develop industry specific generic models, possibly leading to organisational risk scores. Links between process complexity and M-RiCM score could be studied to trigger process simplifications and reengineering. Study on the correlation between the risk control score and compliance could provide information on whether non-compliant organisations could be identified using this score. Methods to harmonise various risks organisations face could be studied using this model to make risk management simpler and efficient. Using technology, particularly virtual reality, expressing the scores in three dimensions could help executives appreciate the risks better. There could be several areas of application of this Model beyond the realm of what this paper has explored.

References

BDO. (2015). Risk Factor Report - Telecommunications.

BDO. (2017). Technology Risk Factor Report.

Carazo J.L., C. J. (2016). Model risk management: quantitative and qualitative aspects. In D. V. Cantino V, Risk management: perspectives and open issues (pp. 491-507). McGraw Hill.

Coleman, T. S. (2011). A Practical Guide to Risk Management. Research Foundation of CFA Institute, USA.

COSO. (2017). Enterprise Risk Management - Integrating with Strategy and Performance - Executive Summary. Retrieved from www.coso.org: https://www.coso.org/Pages/erm-integratedframework.aspx

COSO. (n.d.). COSO Internal Control Framework. Retrieved from https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf

Crouhy M, G. D. (2004). Risk Management. McGraw-Hill.

Dennis Chesley, J. P. (n.d.). Powerful complements: The value of ERM and internal control together. Retrieved from PwC: https://www.pwc.com/gx/en/services/advisory/consulting/risk/resilience/value-of-erm-and-internal-control-together.html

E&Y. (2014). Top 10 risks in telecommunications. Ernst & Young.

Ellul, A. a. (2012). Stronger Risk Controls, Lower Risk: Evidence from U.S. Bank Holding Companies. Journal of Finance, Forthcoming.

IFAC. (2018, August 26). Risk Management & Internal Control. Retrieved from https://www.ifac.org/global-knowledge-gateway/risk-management-internal-control?overview

IIA-IPPF. (n.d.). Retrieved from IIA: https://www.iia.org.uk/resources/ippf/international-standards/glossary/

IIARF. (2014). A Comprehensive Assessment Model (CAM) for Enterprise Risk Management – evaluating internal control systems. Retrieved from https://www.interniaudit.cz/download/IIA/Evaluating-Internal-Control-Systems.pdf

IRMI. (2018, August 26). Risk Management Vs Internal Audit. Retrieved from https://www.irmi.com/articles/expert-commentary/risk-management-versus-internal-control

ISACA. (2013). COBIT 5.0 for Risk. Retrieved from https://cobitonline.isaca.org/

Juneja, P. (n.d.). Risks Faced By Banks. Retrieved from Management Study Guide: https://www.managementstudyguide.com/risks-faced-by-banks.htm

Leitch, M. (2004). Risk Management Vs Internal Controls . IRMI Blog, https://www.irmi.com/articles/expert-commentary/risk-management-versus-internal-control.

Li, Y. P. (2013). Game Analysis of Internal Control and Risk Management . International Journal of Business and Management.

MaGC. (n.d.). LAMP. Retrieved from www.MaGC.in: http://www.magc.in/lamp/

P.O.J.Kelliher, D. W. (2011). A Common Risk Classification System for the actuarial profession. UK: The Institute and Faculty of Actuaries.

PCAOB. (n.d.). Retrieved from AU Section 312 - Audit Risk and Materiality in Conducting an Audit of PCAOB: https://pcaobus.org/Standards/Archived/Pages/AU312.aspx

Reference for Business - Risk Management. (2018, August 26). Retrieved from http://www.referenceforbusiness.com/management/Pr-Sa/Risk-Management.html

Rice C, Z. A. (2018, May-June). Managing 21st Century Political Risk. Harvard Business Review.

Web-search. (2018, August 26). Retrieved from https://searchcompliance.techtarget.com/definition/risk-management

Wikipedia. (2018, August 26). Retrieved from https://en.wikipedia.org/wiki/Risk

About the authors

Praveena K R

MCom, ACA, CISA

Praveena is a Finance and Information Security professional. She is a Chartered Accountant (ACA) and Certified Information Systems Auditor (CISA) by qualification. Praveena has undergone the ISO Lead Auditor course (Information Security Management System) and has a Six Sigma Green Belt. She has over ten years of experience in accounting, auditing and consulting.

Her areas of expertise include Information Systems Audit, IT Security Audit, Internal and Management Audit, Business Process Reengineering, MIS, Business Plans and Feasibility Studies. Her countries of work experience include India, UAE, Bhutan, Bangladesh, Netherlands, and UK.

She is a Senior Consultant at MaGC and can be reached at praveena@magc.in.

Dr R S Murali

PhD (Economics), FCA, ACMA, ACS, CISA, CRISC, DCM (ICA), Programme in Business Process Reengineering, SAP (ERP) FI & CO, Certified Management Consultant – CMC, Certified in Forensic Accounting and Fraud Detection, Certification in Business Excellence for Consultants (SPRINGS Singapore), SPMC - Senior Practicing Management Consultant, Singapore

Dr. R S Murali has over three decades of consulting experience implementing projects for funding agencies such as the World Bank & The Asia Foundation, and for the Indian Government. He has also worked with leading corporate entities, academic institutions, Public Sector Enterprises, and Non-governmental Organizations. He has worked in India, Africa, Singapore, UAE and UK.

Dr. Murali's expertise are in the areas of Public Financial Management, Financial Management, Management Accounting & Costing, Information Technology, Training, and Research.

He along with the team at MaGC have developed various consulting tools out of the rich consulting experience in Government and Private sector. He has published over 25 research articles in professional journals, published three books, and contributed in chapters in five books.

He is Managing Director and Principal Consultant at MaGC and can be reached at muralirs@magc.in.