MGC
GLOBAL RISK ADVISORY LLP

RBIA | Now mandatory for banks, NBFCs, UCBs & HFCs

The Reserve Bank of India has earlier this year expanded the coverage of risk based internal audits ('RBIA')s to specific non-banking financial companies ('NBFC')s, urban co-operative banks ('UCB')s and housing finance companies ('HFC')s.

What is the concept of RBIAs? How does this development impact banking and financial service organizations? Is this relevant to organizations across sectors? What must organizations do to make RBIAs effective?

This thought leadership paper, which contains views of our internal audit experts, explains.

In the words of our Managing Partner *(Monish G Chatrath*) - *It's no longer a cliché, it's a reality and it's here to stay" .*

Context

The concept of risk management has undergone a sea change over the last few years and the industry has come to realize that **inherent in any change initiative is the uncertainty of achieving the intended benefits, which deliver business value.** This uncertainty also requires risk management to be an integral component of an organization's change management approach.

It is organizations that have procedures in place to identify risks as they emerge and introduce systems to manage them, which experience fewer 'sudden shocks' as these risks crystallize. This results in freeing up management time, which would otherwise have been spent in fire-fighting issues that emanate from risks. In the current business environment, **a robust management of risk is also a source of advantage, providing a defense against events impacting the achievement of an organization's objectives and implementation of strategy.**

The **Companies Act 2013** has established specific responsibilities [in the provisions of Section 134 (3)n; Section 177 (4) and Schedule IV referred to by Section 149 (8)] for the **board of directors** ('BoD')s, **audit committees, independent directors** and **management** for the development and institutionalization of an effective **enterprise-wide risk management** ('EWRM') **framework** in their organizations.

Guidelines from The Securities and Exchange Board of India ('SEBI') for listed companies require procedures to inform the BoD of risk assessment and minimization procedures in the organization. The applicability and role of the **risk management committee** has been set out in the '**Amendments to the Securities and Exchange Board of India** (Listing Obligations and Disclosure Requirements) **Regulations'** ('LODR') 2021.

Requirements set out by regulatory bodies

SEBI had prescribed the constitution of a risk management committee, in each of the top 100 companies by market capitalization, which has been subsequently extended to the top 1,000 listed entities by market capitalization in **LODR 2021**.

The **Insurance Regulatory & Development Authority of India** has established a framework for the incorporation and ongoing monitoring of risk assessments for insurance companies.

The RBI had in December of 2002 introduced the concept of RBIA for all scheduled commercial banks *(except regional rural banks).* In February of 2021, the RBI had mandated **select NBFCs with an asset size of INR 5,000 crore and above; and all UCBs with an asset size of INR 500 crore and above to implement their RBIA framework by March 31, 2022**. In June of 2021 the RBI had **extended RBIA to select HFCs** to enhance the quality and effectiveness of their internal audits. While strong governance in NBFCs and UCBs is imperative for the banking and financial services sector, the prevalence of varied approaches to their internal audits has made them susceptible to inconsistencies in application and operations.

Requirements for scheduled banks, NBFCs, UCB's & HFCs

The ongoing deregulation and liberalization of the Indian banking and financial services sector has necessitated the institutionalization of robust risk management and stringent internal control systems in the conduct of banking activities. This aspect is not only a consequence of specific unsavory incidents by some prominent borrowers in the Indian financial market but is also significant in view of the **Basel Capital Accord** under which capital maintained by a bank needs to be more closely aligned to the risks.

Internal audits and risk management

Traditional internal audits have focused on transaction testing, while providing assurance on the reliability of accounting records and financial reports, in addition to the state of compliances with specific legislative requirements. However, the role, merit and impact of **EWRM has over the recent few years become more prominent with it now being viewed as an essential pillar of good governance**.

BoDs, audit committees and the management of organizations are increasingly focusing on identification of their **strategic, operational, financial and compliance risks** and in establishing an effective framework to assess, polarize and mitigate these risks.

In many ways this requires organizations to **go beyond the assessment of the effectiveness of their internal controls over financial reporting** and engage their risk management and/or **internal audit function in providing assurance over the design and operating effectiveness of their risk management systems**.

The **paradigm shift is to an approach that focuses on the evaluation of the risk management systems**, in addition to transaction testing, in a manner that can facilitate proactive anticipation of potential risks and ascertain best practices to mitigate the same.

This makes the internal audit function a cornerstone of governance and consequently requires **the charter and strategy for execution of internal audits to be aligned with the organization's risk management framework**.

Manifest in the approach for RBIAs is an imperative need to first identify those areas that pose the greatest threat to the fulfilment of an organization's objectives, be they internal or external, and then ascertain means of managing them within a cost benefit equation *(after considering the risk appetite and risk tolerance - two specific terms that have also been explained in the COSO 2017 framework)*.

Implementation and ongoing operation of RBIA

Set forth in the ensuing bullets are our recommendations in the form of a phase-wise approach that seeks to make RBIAs effective.

- **Phase 1 |** Assess the risk maturity, appetite and tone at the top.
- **Phase 2 |** Undertake secondary research and subscribe to technical alerts, forums and data bases that provide industry trends, developments and best practices, with current and emerging threats, vulnerabilities and risks.

Implementation and ongoing operation of RBIA (cont…)

- **Phase 3 |** Undertake an independent assessment of risks and polarize these *(i.e. rate the same in their relative importance to the business)* after ascertaining their likelihood & impact at gross and residual levels *(i.e. after considering the impact of mitigating measures)*. Ascertain the determination of the levels *(high, medium, low)* and trends *(increasing, stable, decreasing)* of inherent business risks and control risks. Use data analytic and trend identification*(including AI)* tools, as appropriate.
- **Phase 4 |** Develop a *3-by-3* or *4-by-4* heat map and place activities within cycles in the respective quadrant on the basis of their residual risk polarization.
- **Phase 5 |** Use the heat map to develop a risk driven internal audit charter *(with the nature, extent, manner, type and frequency of testing).*
- **Phase 6 |** The RBIA should include identification of inherent business risks in various activities, evaluation of the effectiveness of the controls for monitoring inherent risks of business activities and in developing a risk-matrix for inherent business risks as well as control risks.
- **Phase 7 |** Undertake an assessment of the status of implementation of previously agreed recommendations and identify the changes *(from previous assessments)* in the polarization of risks.
- **Phase 8 |** The RBIA report should contain adequate, reliable, pertinent and useful information to support observations and conclusions, in addition to recommendations that are practical to implement.

Final thoughts

While the nature of risks across industries are relatively diversified, yet they are inextricably inter-winded. It follows that the **consequences of one risk has a direct impact on several of the others** and such risks relate to emerging practices and innovations within competition, demographic shifts in customer requirements, regulatory & policy intervention, integration with technology, environmental and geopolitical events etc; while others are inherent in threats associated with over reliance on model-based risk management; industry reputation; and the possible emergence of an entirely new market landscape with changed consumer needs and demographics.

Apart from these risks, businesses are also **susceptible to fraudulent conduct**. In our last thought leadership alert we had discussed how the Covid pandemic has provided a fresh breeding ground for fraud risks.

Finally, our experience has revealed that there is no single RBIA framework that can cater to all situations. Consequently, rather than self-imposing frameworks that are published for other organizations, it is **important to first assess the maturity with areas for enhancements in your existing risk management practices and the state of integration of your internal audit functio**n with the risk management strategy of your organization.

It will be more practical for your stakeholders to **adapt to modified forms of existing practices by addressing specific weaknesses in the same** than to a completely new framework.

About MGC Global

Recognized as one of the '10 most promising risk advisory services firms' in 2017, as the 'Company of the Year' in 2018 &, 2019' *(both in the category of risk advisory services),* one of the 'Top Exceptional Companies to Work For' in 2020 and amongst the 'Top 25 Customer Centric Companies' in 2020 and 'The Consultant of the year' in 2021 *(in the category of risk advisory services)*; MGC Global is an independent member firm of the US$ 4.2 billion, Atlanta headquartered - Allinial Global.

MGC Global provides services in the areas of enterprise wide risk management, control assessments *(SOC, IFCR & SOX)*, internal audits, process re-engineering, governance frameworks, IT advisory, GDPR, cyber security, CxO transformation and forensic services. Our Firm has the capabilities to service its clients through its offices in Bengaluru, Mumbai, NCR; and has service arrangements in all major cities in India.

About Allinial Global

Allinial Global *(formerly PKF North America)* is currently the world's second-largest member-based association *(with collective revenues of approximately USD 4.2 billion)* that has dedicated itself to the success of independent accounting and consulting firms since its founding in 1969. It has member firms in 71 countries, who have over 28,000professional staff and over 4,000 partners operating from 688 offices across the globe.

Allinial Global provides its member firms with a broad array of resources and support that benefit both its member firms and their clients in the key impact areas of learning and development, human resources, international outreach, technical support, knowledge-sharing platforms through its specialized communities of practice, marketing resources, information technology and best practices in practice management.