



INTERNAL AUDIT THE WAY FORWARD

BDO India
2025



AN OVERVIEW OF THE CURRENT INTERNAL AUDIT SPACE

Internal audit is an independent and objective function for improving an organisation's processes, mapping mission-critical activities within each process with a layer of preventive and detective controls to add value to the organisation and mitigate the threat of new and emerging risks. An effective system of internal audit evaluates and improves the effectiveness & efficiency of an organisation's risk management systems, control framework, business culture, governance processes including at the top to ensure the organisational goals are accomplished.

In the current unprecedented times, the primary objective of internal audit is to support sustainability of business operations by strengthening the control environment. With the COVID-19 pandemic leading to a sharp rise in home-based working, IT risks centred around the protection of a business' confidential information have increased. There is an onerous responsibility on internal audit functions to enhance the effectiveness of standard operating procedures in the work from home environment, as a disrupted business environment may increase the incidence of uncertainty around business continuity. As we progress, the primary challenge for the internal audit function will be to ensure that they continue to provide secure oversight while adapting to a dynamic risk landscape.



COLLABORATIVE AND INTEGRATED APPROACH FOR EFFECTIVE INTERNAL AUDIT

Internal audit teams are adding tremendous value by shouldering additional responsibilities in the identification of threats, vulnerabilities, disaster management, and business continuity thereby ensuring that the incidence of business, strategic, operational, financial reporting, reputational, and information technology risks are minimised. While the Audit Committee and Board of Directors provide overall direction and oversight, the **'three lines of defence'** provide a simple and effective way to enhance communications by clarifying roles and duties. The three lines of defence are essentially the three control authorities within the organisation involved in effective risk management:



FIRST-LINE - FUNCTIONS THAT OWN AND MANAGE RISKS

The first line is responsible for setting up the controls, mitigating risks and defining policies and procedures to be complied with. As the first line of defence, operational managers own and manage risks. They also are responsible for implementing corrective actions to address process and control deficiencies.



SECOND-LINE - FUNCTIONS THAT OVERSEE RISKS

The second line monitors compliance in accordance with the laid down controls. It is not an independent assurance function, but a monitoring tool for the management. The management establishes separate functions such as Risk Management Committee (monitors the implementation of effective risk management practices), Compliance Function (monitors risks emanating from non-compliance with applicable laws and regulations), and Controller Function (monitors financial risks and financial reporting issues), as a second line of defence to monitor the first line of defence.



THIRD-LINE - FUNCTIONS THAT PROVIDE INDEPENDENT ASSURANCE

The third line provides independent assurance on the activities of the first and second lines of defence. Internal auditors provide the governing body and the senior management with comprehensive assurance based on the highest level of independence and objectivity within the organisation.

INTERNAL AUDIT AND ITS COLLABORATION WITH ICOFR, ERM, ITGC, AND AI FOR ENHANCING EFFECTIVENESS



INTERNAL CONTROLS OVER FINANCIAL REPORTING (ICOFR)

ICOFR is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements in accordance with generally accepted accounting principles

Integration of internal audit with the ICOFR test of design and operating effectiveness addresses 5 key financial statement assertions:

- Existence or occurrence
- Completeness
- Rights and obligations
- Valuation or allocation
- Presentation and disclosure

Objectives

Internal controls should provide reasonable assurance to achieve the following objectives:

- Effectiveness and efficiency of operations (including safeguarding fixed assets)
- Reliability of financial reporting
- Compliance with applicable laws and regulations

Evaluation levels

Internal controls must be evaluated at three levels viz. entity level, process level, and information technology automation level.

Components:

The components of internal controls mapped to the following five broad heads enhance the internal audit function:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring



ENTERPRISE RISK MANAGEMENT (ERM)

ERM is the process of identifying and documenting the potential incidents that may represent the new and emerging risks to the achievement of the organisation's strategic objectives.

The Committee of Sponsoring Organisations (COSO) in September 2017, updated its ERM framework defining the concepts of 'Risk Appetite' and 'Risk Tolerance'. While risk appetite is the amount of risk an entity is willing to accept in the pursuit of its strategy and business objectives, risk tolerance is the acceptable level of variation relative to the achievement of a specific objective.

The COSO ERM framework is integrated with the internal control environment providing specific guidance on the following attributes during internal audit engagements:

- Internal environment: Tone at the top, risk appetite, values
 - Objective setting: Establish objectives and strategies
 - Event identification: Internal and external risks and opportunities
 - Risk assessment: Probability and impact assessment
 - Risk response: Risk mitigation plan
-



INFORMATION TECHNOLOGY GENERAL CONTROLS (ITGC)

ITGCs are designed for application to the IT systems such as applications, operating systems, databases, and supporting IT infrastructure including cloud-based IT support. The objectives of ITGCs are to ensure the integrity of the data and processes that the systems support.

Testing the design and operating effectiveness of ITGC is extremely important for organisations as highly confidential and entity-specific sensitive information rests on secured gateways, data farms, and servers which are vulnerable to data security attacks and threats.

Cyberattacks such as the very recent one ‘Wannacry Ransomware’ are unpredictable and at times leave the enterprises unprepared to combat the resultant risks associated with them. A cyberattack can be extremely fatal for any enterprise since it denotes susceptible intrusion/ breach of security thereby endangering the security of pivotal information and, through it, the financial position, operational strategy, vision, and mission, and more importantly, the trust and reputation the organisation has established since its inception.

The tone at the top is clear with an increasing sense of expectation from the internal audit function to assess the enterprise’s attributes in managing such associated risks.



ARTIFICIAL INTELLIGENCE (AI)

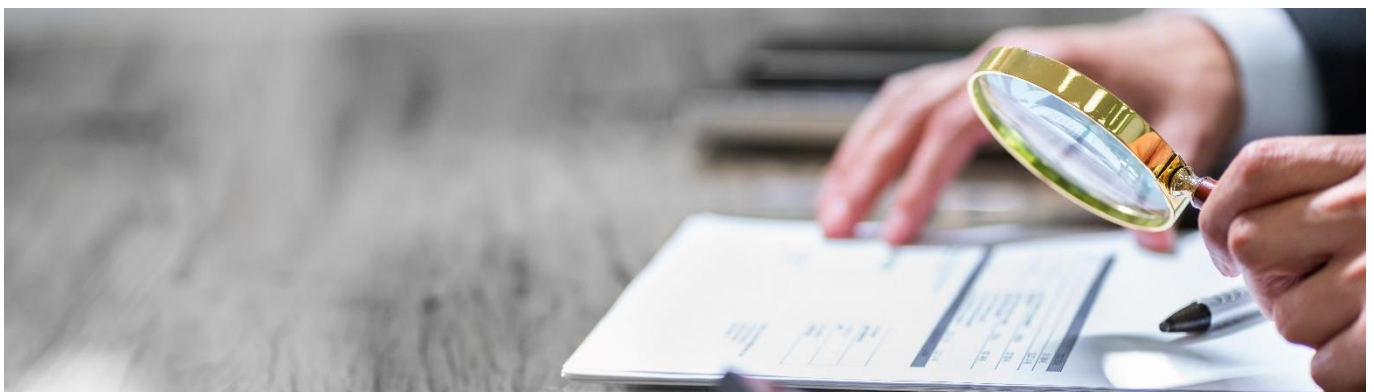
AI is the ability of a machine integrated with robotic process automation to perform tasks by way of simulation of human intelligence. AI systems work by analysing big data for correlations and patterns and using intelligence to forecast future trends/ values.

AI tools are audit analytics software platforms that utilise machine-learning artificial intelligence to uncover errors, including material irregularities and/or anomalous transactions. Such tools assist in the performance of key internal audit procedures such as:

- Data analytics
- Quantification of financial impact
- Extrapolation of quantified results
- Segregating information beyond the materiality for greater insights

AI makes the internal audit process faster, more accurate, and complete, resulting in lower risk exposure and providing clients with complete assurance that exceeds regulatory and industry standards. The key features of AI which integrate with the internal audit function thereby making it more effective include:

- Out-of-the-box integration with leading ERPs and accounting software resulting in big data analytics
- Intelligent transaction sampling
- Intuitive user interface design that does not require scripting
- Advanced machine-learning & rules-based control points
- Risk-based scoring
- Data science-based anomaly detection



CONCLUSION

As we look ahead, several trends will influence the internal audit function. Some of these are:

Dealing with proliferation of data

As more data becomes available and the speed at which new data can be analysed increases, internal audit will need to adapt. The data will be churned from both inside and outside the entity and will be structured in new ways. Advanced analytics and data visualisation tools will evolve and be very helpful in understanding risk and its impact.

Leveraging AI and Automation

We have entered the era of automated processes and AI. Regardless of individual beliefs, internal audit practices need to consider the impact of these and future technologies and leverage their capabilities. Previously unrecognisable relationships, trends, and patterns could be uncovered, providing a rich source of information critical to managing risk.

Building stronger organisations

As organisations become better at integrating internal audit with strategy and performance, an opportunity to strengthen resilience will present itself. By knowing risks that will have greatest impact on the entity, organisation can use the internal audit function to help put in place capabilities that allow them to act early. This will open new opportunities.

Managing the cost of risk management

As ERM practices evolve, it will become important that activities spanning risk, compliance, control, and even governance be efficiently coordinated to provide maximum benefit to the organisation. This may represent one of the best opportunities for the internal audit function to redefine its importance to the organisation.

For any content related queries, kindly get in touch with,

LAV GOYAL

Partner & Head
Business Advisory Services
lavgoyal@bdo.in

TARUN KHER

Partner/ Risk and Advisory Services
Business Advisory Services
tarunkher@bdo.in

For any other queries or feedback, kindly write to us at marketing@bdo.in

BDO Global

BDO is an international network of independent public accounting, tax and advisory firms. We support organisations with an unwavering focus on quality, industry expertise, and the innovative use of technology to deliver impactful solutions. Our commitment to people, clients, and communities is at the core of everything we do. With our people-first culture, we foster an environment where diversity thrives, growth is nurtured, and continuous learning drives lasting progress for a sustainable future.

BDO India

BDO India offers Assurance, Tax, Advisory, Technology Products & Solutions, Digital Transformation, and Managed Services & Outsourcing to domestic and international clients across various industries. Bringing together expertise, innovatively driven and delivered through technology, we empower businesses to navigate their unique challenges with transformative, impactful, client-centric solutions. The team in India comprises over 11,000* professionals, led by more than 350 Partners and Directors, operating out of 20 offices across 14 key cities.

*Includes employees from BDO RISE and BDO EDGE

Ahmedabad | Bengaluru | Bhopal | Chandigarh | Chennai | Coimbatore | Delhi | Goa | Hyderabad | Kochi | Kolkata | Mumbai | Pune | Vadodara

This publication has been carefully prepared, but it has been written in general terms and should be seen as containing broad statements only. This publication should not be used or relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained in this publication without obtaining specific professional advice. Please contact BDO India Services Private Limited to discuss these matters in the context of your particular circumstances. BDO India Services Private Limited, its directors, promoters, employees and agents do not accept or assume any responsibility or duty of care in respect of any use of or reliance on this publication, and will deny any liability for any loss arising from any action taken or not taken or decision made by anyone in reliance on this publication or any part of it. Any use of this publication or reliance on it for any purpose or in any context is therefore at your own risk, without any right of recourse against BDO India Services Private Limited or any of its directors, promoters, employees or agents.

BDO India Services Private Limited, a private limited company incorporated in India, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member entities.

BDO is the brand name for the BDO network and for each of the BDO Member Entities

Copyright © 2025 BDO India Services Private Limited. All rights reserved. Published in India.

Visit us at www.bdo.in

