

THE POWER OF BEING UNDERSTOOD



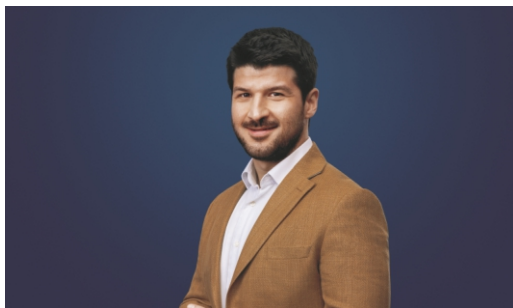
Hien

One of the
RSM team



Internal Audit in the New Era of Governance





RSM IN INDIA

- RSM India (comprising of RSM Astute Consulting Group and affiliates) is consistently ranked amongst India's top tax, accounting and consulting groups [International Accounting Bulletin – India Surveys]
- Nationwide presence through offices in 13 key cities across India
- Multi-disciplinary personnel strength of over 3,000
- International delivery capabilities

rsmindia.in

RSM AROUND THE GLOBE

- Amongst world's leading provider of audit, tax and consulting services to entrepreneurial growth-focused organisations globally
- Annual combined fee income of US\$ 9.4 billion
- Combined staff of over 64,000 in over 820 offices across more than 120 countries

rsm.global



Internal Audit in the New Era of Governance



“Business will be better or worse. We cannot do today’s job with yesterday’s methods and be in business tomorrow.”

– Nelson Jackson

The role of Internal Audit in governance has undergone complete transformation in the past decade and continues to undergo improvisation, innovation and digital transformation. For most large and mid-sized organizations as well as NewAge businesses, internal audit is backbone of governance in the modern era. The primary reasons for this can be summarised as follows:

- Regulatory Requirements for Internal Audit under the Companies Act, 2013 and the rules framed thereunder, the Reserve Bank of India regulations as updated in 2021 and 2022, the Insurance Regulatory & Development Authority and other regulations
- Heightened Governance Expectations of Stakeholders such as investors, lenders, regulators, business partners and other stakeholders
- Governance crucial element of ESG and SEBI's regulations regarding BRSR Core and third-party assurance announced in 2023
- Better Valuations and Access to Capital and governance “premium”
- Reputational Risk due to extensive requirements of reporting for frauds and misreporting both under the Companies Act and the SEBI regulations and the spiraling impact of the print, electronic and social media
- Size and Scale of Organisations as well as Meteoric Rise of Indian Businesses as Indian companies having annual revenues exceeding Rs. 200 crores (about US\$ 25 million) require mandatory internal audit.
- Rise of NewAge Businesses

In view of the above, Internal Audit function plays a very crucial role in an organisation's corporate governance framework, internal processes and controls, risk management,

Preface

regulatory compliance, financial & ESG reporting and overall assisting the Board of Directors and senior management enabling them to fulfil their responsibilities towards the organisation and its stakeholders.

The professional bodies for internal audits have issued standards which provide valuable guidance and structured approach for acceptance, planning, conduct, reporting and documentation of Internal Audits. The ICAI has issued the following standards:

Series	Standard No	Title
100 Series: Standards on Key Concepts	SIA 110	Nature of Assurance
	SIA 120	Internal Controls
	SIA 130	Risk Management
	SIA 140	Governance
	SIA 150	Compliance with Laws and Regulations
200 Series: Standards on Internal Audit Management	SIA 210	Managing the Internal Audit Function
	SIA 220	Conducting Overall Internal Audit Planning
	SIA 230	Objectives of Internal Audit
	SIA 240	Using the Work of an Expert
	SIA 250	Communication with Those Charged with Governance
300–400 Series: Standards on the Conduct of Audit Assignments	SIA 310	Planning the Internal Audit Assignment
	SIA 320	Internal Audit Evidence
	SIA 330	Internal Audit Documentation
	SIA 350	Review and Supervision of Audit Assignments
	SIA 360	Communication with Management
	SIA 370	Reporting Results
	SIA 390	Monitoring and Reporting of Prior Audit Issues
500 Series: Standards on Specialized Areas	SIA 520	Internal Auditing in an Information Technology Environment
	SIA 530	Third Party Service Provider
Standards Issued up to July 01, 2013	SIA 5	Sampling
	SIA 6	Analytical Procedures
	SIA 7	Quality Assurance in Internal Audit
	SIA 11	Consideration of Fraud in an Internal Audit
	SIA 18	Related Parties

Preface

This role is ever expanding and in many matured organisations, it is expected that the role of Internal Audit function must spread into newer and broader areas such as sharing data driven insights for management's strategic and transformative plans, monitoring actual progress for key management initiatives, real time compliance dashboards and revenue optimisation and cost. With the increased focus on analytics, automation, artificial intelligence and technology tools, Internal Audit function can act as an intelligent and agile tool for trends, triggers and preventive actions on a real time basis.

The Chief Audit Executive is expected to venture into newer areas and keep innovating and improvising its Audit Charter so that the value and benefits to the organisation are maximised. Thus, there is a definitive shift in perception of Internal Audit function from being a 'Cost Centre' to being a 'Profit Centre'.

In this booklet, we have endeavoured to touch upon the key aspects of internal audit and the role of Internal Audit in the ever-changing business environment and digital arena. We have discussed the role of Internal Audit in governance, standards on Internal Audit, current regulatory framework around Internal Audit and corporate governance. This follows by some insights on how Internal Audit function has joined the transformation bandwagon leveraging experts and technology, analytics and automation. Finally, we cover the reporting and communication with stakeholders for the Internal Audit function.



We hope you find this publication relevant and useful.

Happy Reading!

Table of Contents

Contents	Particulars	Page
Chapter 1	Internal Audit & Governance	1
1.1	Internal Audit – Reasons for Transformation	1
1.2	In Internal Audit – Transformation Journey	3
1.3	Brief comparison of Traditional, Risk Based and Modern Internal Audit	4
1.4	Internal Audit – India Perspective	4
1.5	Current Trends in Internal Audit	6
1.6	Upcoming Trends	7
1.7	Upcoming Challenges	8
Chapter 2	Standards on Internal Audit (Global and ICAI Pronouncements)	9
2.1	Why Are These Standards Crucial	9
2.2	Global Standards: The IPPF Framework	10
2.3	ICAI's Standards on Internal Audit (SIAs)	11
2.4	A brief overview of SIA framework	12
2.5	Detailed overview of each SIA	14
Chapter 3	Regulatory Framework – Internal Audit	21
3.1	Company Law Regulation	21
3.2	Implementation of Other Frameworks	23
3.3	Other Important Regulatory Aspects	24
3.4	RBI Regulations	28
Chapter 4	Expectations from Internal Audit	37
4.1	Key Stakeholders' Expectations from IA	39
4.2	Necessity of Internal Auditor to meet the Audit Committee of the Board	42
Chapter 5	Role of Subject Matter Experts in enhancing value proposition of IA	46
5.1	Defining a Subject Matter Expert	46
5.2	Enhancing Role of Internal Audit by involving Subject Matter Experts	47

Table of Contents

Contents	Particulars	Page
5.3	Integrating Subject Matter Experts into the Audit Process	48
5.4	Best Practices for Collaborating with SMEs	54
5.5	Strategies for identifying the relevant SMEs	56
5.6	Challenges in Utilising SMEs	58
5.7	Key Areas requiring SMEs	58
Chapter 6	Role of Analytics, Automation and Artificial Intelligence (AAA) in Internal Audit	66
6.1	Data Analytics Enabled Automation	66
6.2	Artificial Intelligence in Internal Audit	70
6.3	Tools Deployed for Analytics and Automation in Internal Audit	77
6.4	Auditing in an Artificial Intelligence Environment	79
Chapter 7	Technology Impact and Changing Dynamics of Internal Audit	81
7.1	Information Technology in Internal Audit – A Key Differentiator	82
7.2	Key IT Considerations for Internal Audit	83
7.3	Digital Personal Data Protection Act, 2023	91
Chapter 8	Internal Audit Reporting	102

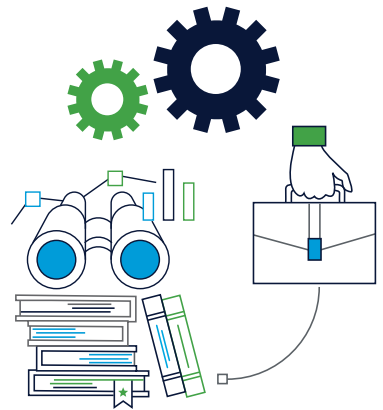
The role of Internal Audit in governance has undergone complete transformation in the past decade and continues to undergo improvisation, innovation and digital transformation. For most large and mid-sized organizations as well as NewAge businesses, internal audit is backbone of governance in the modern era.

1.1 Internal Audit – Reasons for Transformation

The primary reasons for the transformation of internal audit can be enumerated as follows:

1.1.1. Regulatory Requirements

The Companies Act, 2013 and the rules framed thereunder provided statutory recognition to the role of the internal audit by making it mandatory for most large and mid-sized companies, defining the role of audit committee and the board regarding internal audit, the scope and reporting mechanism and so on. The Reserve Bank of India has stipulated regulations regarding internal audit, concurrent audit, risk management for banks and Non-Banking-Finance Companies. The Insurance Regulatory & Development Authority and other regulators have also recognized the role of internal audit and provided for the regulations for the sectors they are entrusted.



1.1.2. Heightened Governance Expectations of Stakeholders

The expectations of investors, lenders, regulators, business partners and other stakeholders have increased more than ever before in terms of safeguarding assets and business, internal controls, risk management, compliances, fraud risk management and the reputation of the organisation.

1.1.3. Governance Crucial Element of ESG

The unprecedented significance of Environment, Social and Governance aspects in the conduct of business is evident from SEBI's regulations regarding BRSR Core

and third party assurance announced in 2023. The stock exchanges across the globe are now rating companies on ESG score (NSE and Dow Jones)

1.1.4. Better Valuations and Access to Capital

It is evident that the companies with better governance are able to command better valuation and access capital. Internal audit plays an important role in this and avoiding possible frauds, misreporting, loss of assets and reputation. There is a governance "premium" such companies command over their peers.

1.1.5. Reputational Risk

The extensive requirements of reporting for frauds and misreporting both under the Companies Act and the SEBI regulations pose the reputational risks from such incidents which internal audit endeavours to prevent. The stock exchange reports are readily picked up by the print, electronic and social media creating a spiraling impact. The recent incidents of a leading coffee chain, e-learning company and large businesses are testimony of this.

1.1.6. Size and Scale of Organisations

The organizations are now much larger with several Indian companies having annual revenues exceeding Rs. 200 crores (about US\$ 25 million) which is the threshold for mandatory internal audit. Further, there are hundreds of businesses with over Rs.1,000 crore revenue company. This size and scale warrant the need for an objective and constructive internal audit function.

1.1.7. Meteoric Rise of Indian Businesses

The Indian businesses have seen meteoric rise with several Indian companies now valued at over Rs.1,000 crores or even Rs. 10,000 crores. This is across industries such as technology, pharmaceuticals, manufacturing, consumer goods, infrastructure, banking and financial services, digital businesses and so on.

1.1.8. NewAge Businesses

The role of internal audits in NewAge businesses can hardly be exaggerated. These are businesses which are growing at break neck speed and are digitally driven with sometimes poorly defined processes and controls with high people attrition which

can be breeding ground for frauds, lapses and losses.

In view of the above, Internal Audit function plays a very crucial role in an organisation's corporate governance framework, internal processes and controls, risk management, regulatory compliance, financial & ESG reporting and overall assisting the Board of Directors and senior management enabling them to fulfil their responsibilities towards the organisation and its stakeholders.

The professional bodies for internal audits have issued standards which provide valuable guidance and structured approach for acceptance, planning, conduct, reporting and documentation of internal audits.

This role is ever expanding and in many matured organisations, it is expected that the role of Internal Audit function must spread into newer and broader areas such as sharing data driven insights for management's strategic and transformative plans, monitoring actual progress for key management initiatives, real time compliance dashboards and revenue optimisation and cost. With the increased focus on analytics, automation, artificial intelligence and technology tools, Internal audit function can act as an intelligent and agile tool for trends, triggers and preventive actions on a real time basis.

1.2. Internal Audit – Transformation Journey

In the past, Internal Audit (IA) had limited focus and aimed more at safeguarding assets, reliability of financial statements and keeping watch on potential financial mismanagement. With the phenomenal growth in the businesses and operations across multiple geographies, internal audit became essential in risk management, better corporate governance, compliance with regulations and internal procedures and supporting management in higher operational efficiency. The role of internal audit is evolving with changes in existing businesses, emerging of new businesses, technological and regulatory developments etc.,

The modern internal auditing extends to pro-active participation with management, providing recommendations, and identifying potential issues before they escalate, thereby supporting organizational growth. The role has developed into assessment of business risks, assurance on controls, efficiency in operations, etc.

1.3. Brief comparison of Traditional, Risk Based and Modern Internal Audit

Era	Traditional Method	Risk-Based Auditing	Modern Internal Audit
Key Focus	Compliance, error detection, financial accuracy	Operational efficiency, fraud prevention, governance	Strategic role, continuous auditing, data-driven insights
Technologies Introduced	Manual methods, paper-based processes	ERP systems, data analytics, internal control systems	AI, machine learning, data visualization tools, continuous auditing, RPA, blockchain
Auditing Methodology	Reactive, limited scope	Proactive, risk-based, aligned with business strategy	Real-time insights, data-driven decision-making
Limitations / Benefits	Time-consuming, prone to human errors	Enhanced fraud prevention, operational insights	Improved risk management, operational excellence, real-time insights

1.4. Internal Audit – India Perspective

In India, post globalization and liberalization reforms in 1991, the internal audit function has come a long way since its inception and has undergone significant development in recent years. In the past, internal audit in India was confined to compliance-based activities and was often viewed as a cost center. With the increasing complexity of business operations and the emergence of new risks, however, the role of internal audit in India has evolved to become more strategic in nature.

In India, in line with global standards, IA has started focusing more on reducing risks and improving how things run within companies. Further, the advent of new age

technologies and ERPs (SAP, Oracle, and others) made it easier to do real-time, digital audits.

Some of the important developments in IA function in India are given as below:

- **Increased emphasis on risk management** – The role of risk management in internal audit has significantly enhanced with greater expectations from Internal Audit in reviewing the Risk Management processes and suggest improvements.
- **Increased focus on corporate governance** – With the growing importance of corporate governance in India, internal auditors are now expected to provide assurance on the effectiveness of the organization's governance processes and to make recommendations for improvement. This includes assessing the effectiveness of the board of directors, senior management, and internal controls.
- **Increased focus on technology** – This has also played a significant role in the development of internal audit in India. The rapidly changing technology and use of technological tools have become an integral part of internal audit.
- **Increased focus on sustainability and responsible business practices** – This is yet another development that has had an important impact on the internal audit function in India. There are now regulatory requirements also towards sustainability and responsible business practices.



- **Role of Internal Auditors have evolved and now more aligned with organizational interests and success:**

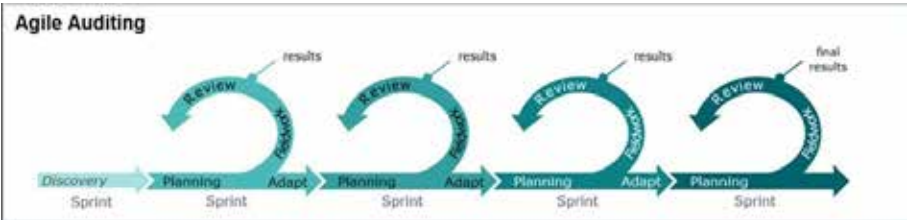
Business Applications and Benefits of Credit Data Science



Source: [https:// fastercapital.com](https://fastercapital.com)

1.5. Current Trends in Internal Audit

1.5.1. Agile Auditing: This methodology employs brief, iterative cycles to continuously deliver value and swiftly adapt to changing circumstances. By maintaining a flexible approach, organizations can respond more effectively to emerging challenges and opportunities.



Source: <https://www.linkedin.com/pulse>

1.5.2. Modern Auditing techniques – Data Analytics (DA) and continuous auditing have really changed how internal audits work nowadays. Frameworks like Internal Control Framework (ICF) and Enterprise Risk Management (ERM) have also helped improve how companies manage risks. Now, internal audits pay more attention to corporate governance, preventing fraud, and making decisions based on data.

- 1.5.3. Data-driven decision-making** – has become a cornerstone of modern internal auditing. By utilizing advanced analytics and AI, auditors can provide management with valuable insights that inform strategic decisions. This data-driven approach ensures that decisions are based on accurate and timely information, enhancing the overall effectiveness of the organization.
- 1.5.4. Cybersecurity and Digital Threats** – These audits identify digital vulnerabilities, ensure compliance with security regulations, and safeguard against cyber-attacks. By proactively addressing potential threats, organizations can enhance their cybersecurity posture and mitigate risks.
- 1.5.5. Sustainability and ESG** – Auditors evaluate the company's management of environmental, social, and governance (ESG) issues, ensuring compliance with ESG regulations and promoting responsible practices. This comprehensive review helps organizations align their operations with stakeholder expectations and regulatory requirements, fostering long-term sustainability and corporate responsibility.
- 1.5.6. Operational Audit** – In addition to financial audits, the internal audit scope is significantly enhanced by addition of operational areas for enhanced value additions.
- 1.6. Upcoming Trends:**
- 1.6.1. AI and Machine Learning:** These tools help auditors spot potential issues before they happen by analyzing past data and finding trends. This makes audits more efficient and accurate.



1.6.2. Blockchain Technology: Blockchain technology ensures transparency and integrity in transactions due to its decentralized and immutable nature. This allows auditors to verify records in real-time, significantly reducing the risk of fraud and enhancing trust in financial reporting.

1.6.3. Real-Time Data Visualization Tools: Advanced visualization platforms enable auditors to continuously monitor financial and operational data. These tools facilitate the immediate detection of anomalies, enhance decision-making processes, and ensure prompt resolution of discrepancies.

1.7. Upcoming Challenges

1.7.1. Keeping Up with Technology: Rapid technological advancements necessitate continuous learning and skill development for auditors. Emerging technologies such as AI, blockchain, and cloud computing require auditors to adopt sophisticated methods for risk assessment. Failure to stay current with these innovations may result in overlooked risks or inefficient practices.

1.7.2. Regulatory Compliance: Regulatory requirements frequently evolve across various industries and regions. Auditors must remain informed about these changes to avoid penalties, safeguard their reputation, and prevent operational disruptions. This is particularly critical in highly regulated sectors such as banking and pharmaceuticals, where compliance standards are stringent.

1.7.3. Talent Crunch & Skill Gaps: There is a notable shortage of skilled auditors, particularly in specialized areas such as data analytics, cybersecurity, and risk management. Modern auditing demands a combination of technological proficiency and traditional expertise, making it challenging to attract and retain qualified professionals. Additionally, training existing staff to meet these evolving requirements imposes an extra burden on organizations.

Internal Audit Standards offer a structured framework that governs how internal audits should be conducted. These standards help ensure that internal auditors maintain a consistent approach to planning, execution, and reporting, thereby adding value to their organizations. Additionally, these standards promote transparency and accountability, helping organizations to identify and mitigate risks more effectively. The structured approach also facilitates continuous improvement in audit practices, ensuring that internal audits remain relevant and aligned with evolving business needs and regulatory requirements.

2.1 Why Are These Standards Crucial?



- **Professional Excellence:** Ensures audits are conducted with the highest standards of professionalism.
- **Consistency:** Establishes uniformity across audits, regardless of the organization or industry.
- **Risk Mitigation:** Enhances the ability to identify and address risks proactively.
- **Regulatory Compliance:** Aligns audit practices with legal and regulatory requirements.

- **Value Addition:** Improves organizational governance, operational efficiency, and strategic decision-making.

2.2 Global Standards: The IPPF Framework

The International Standards for the Professional Practice of Internal Auditing (IPPF), established by the Institute of Internal Auditors (IIA), set the global benchmark for internal auditors. The framework includes several key components:

2.2.1. Core Principles

These principles define the essential qualities for effective internal auditing, such as integrity, objectivity, competence, and alignment with organizational strategies. They ensure that internal auditors provide valuable insights and assurance.

2.2.2. Code of Ethics

The Code of Ethics outlines guidelines for professional conduct, emphasizing integrity, objectivity, confidentiality, and competency. It consists of principles and rules of conduct that internal auditor must adhere to, ensuring ethical behaviour and professionalism.

2.2.3. Standards

The IPPF Standards are categorized into:

- **Attribute Standards:** Focus on the characteristics of organizations and individuals performing internal audits, including independence and proficiency.
- **Performance Standards:** Describe the nature of internal auditing and provide criteria for measuring performance, covering aspects like planning and communicating audit results.
- **Implementation Standards:** Specific to assurance and consulting services.

By adhering to these principles, codes, and standards, internal auditors enhance

governance, risk management, and control processes within their organizations.

2.3. ICAI's Standards on Internal Audit (SIAs)

The Standards on Internal Audit (SIA) issued by the Institute of Chartered Accountants of India (ICAI) provide a comprehensive framework to enhance the quality and consistency of internal audit practices.

ICAI Standards evolved over a period of past 3 decades. A brief history of SIA is as under:

- **Early 2000s:** The Institute of Chartered Accountants of India (ICAI) recognized need for a structured framework for internal auditing. This led to the establishment of the Internal Audit Standards Board (IASB).
- **2004:** The first set of Standards on Internal Audit (SIA) was issued. These initial standards laid the foundation for internal audit practices in India.
- **2007:** The ICAI issued additional standards to cover more specific aspects of internal auditing, reflecting the evolving needs of the profession.
- **2010:** A significant revision of the SIAs was undertaken to align them with international best practices and to address new challenges in the business environment.
- **2013:** The ICAI introduced standards focusing on risk management and internal controls, emphasizing the importance of these areas in internal auditing.
- **2017:** Further updates were made to the SIAs to incorporate changes in regulatory requirements and to enhance the comprehensiveness of the standards.
- **2020:** The ICAI issued new standards and revised existing ones to ensure



they remained relevant in the face of rapid technological advancements and changing business landscapes.

- **2023:** The most recent updates to the SIAs were made, reflecting the latest developments in internal audit practices and regulatory expectations.

As of now, SIAs cover a wide range of topics, including risk management, internal controls, governance, and compliance. The standards are periodically updated to reflect changes in the business environment and regulatory requirements. The ICAI continues to issue new standards and revise existing ones to ensure they remain relevant and effective.

The SIAs are applicable to all internal audit engagements conducted by members of the ICAI. They provide a robust framework that helps internal auditors perform their duties with consistency and quality. These standards are essential for ensuring that internal audits are conducted in a manner that meets the expectations of stakeholders and complies with regulatory requirements. Though these standards are not mandatory as on date, by adhering to these standards, internal auditors can enhance the credibility and reliability of their audit findings, thereby contributing to better governance and risk management within organizations.

2.4. A brief overview of SIA framework is given below:

The 100 Series focuses on fundamental concepts such as internal controls and risk management, while the 200 Series addresses the strategic management of the internal audit function, including planning and communication with governance bodies.



The 300–400 Series covers the execution of audit assignments, detailing aspects like audit evidence, documentation, and reporting to ensure thorough and reliable audits.

Additionally, the 500 Series includes specialized standards for areas such

as auditing in an information technology environment and using third-party service providers. Adherence to these standards helps internal auditors maintain professionalism and contribute to improved governance and risk management within their organizations.

List of SIAs given as below:

Series	Standard No	Title
100 Series: Standards on Key Concepts	SIA 110	Nature of Assurance
	SIA 120	Internal Controls
	SIA 130	Risk Management
	SIA 140	Governance
	SIA 150	Compliance with Laws and Regulations
200 Series: Standards on Internal Audit Management	SIA 210	Managing the Internal Audit Function
	SIA 220	Conducting Overall Internal Audit Planning
	SIA 230	Objectives of Internal Audit
	SIA 240	Using the Work of an Expert
	SIA 250	Communication with Those Charged with Governance
300–400 Series: Standards on the Conduct of Audit Assignments	SIA 310	Planning the Internal Audit Assignment
	SIA 320	Internal Audit Evidence
	SIA 330	Internal Audit Documentation
	SIA 350	Review and Supervision of Audit Assignments
	SIA 360	Communication with Management
	SIA 370	Reporting Results
	SIA 390	Monitoring and Reporting of Prior Audit Issues
500 Series: Standards on Specialized Areas	SIA 520	Internal Auditing in an Information Technology Environment
	SIA 530	Third Party Service Provider
Standards Issued up to July 01, 2013	SIA 5	Sampling
	SIA 6	Analytical Procedures
	SIA 7	Quality Assurance in Internal Audit
	SIA 11	Consideration of Fraud in an Internal Audit
	SIA 18	Related Parties

2.5. Below is a detailed overview of each SIA:

■ 100 Series: Standards on Key Concepts

➤ SIA 110: Nature of Assurance

- Focuses on the concept and scope of assurance in internal audit engagements.
- Emphasizes the need for objective and independent evaluations.
- Highlights how assurance enhances organizational governance, risk, and control processes.

➤ SIA 120: Internal Controls

- Guides auditors on assessing the design and operational effectiveness of internal controls.
- Encourages identifying control gaps and suggesting improvements.
- Emphasizes documentation and reporting of control deficiencies.

➤ SIA 130: Risk Management

- Provides a framework for evaluating risk management processes within organizations.
- Focuses on aligning audit activities with identified risks.
- Recommends proactive measures for mitigating business and operational risks.

➤ SIA 140: Governance

- Stresses the importance of governance structures and

processes in achieving organizational objectives.

- Guides auditors on assessing board effectiveness and decision-making.
- Encourages transparency and accountability in governance practices.

➤ **SIA 150: Compliance with Laws and Regulations**

- Focuses on ensuring compliance with applicable legal and regulatory frameworks.
- Guides auditors to identify non-compliance risks and their implications.
- Highlights proactive measures to prevent legal or reputational issues.

■ **200 Series: Standards on Internal Audit Management**

➤ **SIA 210: Managing the Internal Audit Function**

- Defines the responsibilities of internal audit leaders in managing the function effectively.
- Emphasizes strategic planning, resource allocation, and performance evaluation.
- Promotes alignment with organizational goals and priorities.

➤ **SIA 220: Conducting Overall Internal Audit Planning**

- Guides auditors on creating comprehensive audit plans.
- Recommends prioritizing audits based on risk assessment.
- Emphasizes flexibility to adapt plans to emerging risks.

➤ **SIA 230: Objectives of Internal Audit**

- Clarifies the primary objectives of internal audits, such as adding value and improving operations.
- Focuses on ensuring the reliability of financial and operational data.
- Encourages enhancing governance, risk management, and control processes.

➤ **SIA 240: Using the Work of an Expert**

- Provides guidance on when and how to rely on external experts during audits.
- Emphasizes assessing the competence and objectivity of the expert.
- Recommends clear documentation of expert contributions in audit reports.

➤ **SIA 250: Communication with Those Charged with Governance**

- Highlights the importance of effective communication with governance bodies.
- Recommends periodic updates on audit progress and significant findings.
- Stresses transparency to build trust and ensure accountability.

■ **300–400 Series: Standards on the Conduct of Audit Assignments**

➤ **SIA 310: Planning the Internal Audit Assignment**

- Provides a structured approach to planning individual audit

assignments.

- Emphasizes understanding the audit area and setting clear objectives.
- Stresses resource allocation and time management.

➤ **SIA 320: Internal Audit Evidence**

- Guides auditors on gathering sufficient and appropriate evidence.
- Emphasizes the reliability and relevance of evidence.
- Focuses on ensuring evidence supports audit findings and conclusions.

➤ **SIA 330: Internal Audit Documentation**

- Outlines best practices for maintaining comprehensive and accurate audit records.
- Stresses documentation as evidence of the audit process and findings.
- Highlights its role in facilitating reviews and quality assurance.

➤ **SIA 350: Review and Supervision of Audit Assignments**

- Emphasizes the need for supervision during audit assignments.
- Recommends periodic reviews to ensure adherence to audit standards.
- Focuses on quality control and professional development.

➤ **SIA 360: Communication with Management**

- Encourages continuous engagement with management throughout the audit.
- Recommends discussing preliminary findings and recommendations.
- Focuses on resolving issues collaboratively.

➤ **SIA 370: Reporting Results**

- Guides auditors on presenting audit findings effectively.
- Stresses clarity, conciseness, and action-oriented recommendations.
- Encourages follow-up mechanisms to ensure implementation.

➤ **SIA 390: Monitoring and Reporting of Prior Audit Issues**

- Provides a framework for tracking and reporting unresolved audit issues.
- Emphasizes accountability for addressing recommendations.
- Recommends regular updates to management and governance bodies.

■ **500 Series: Standards on Specialized Areas**

➤ **SIA 520: Internal Auditing in an Information Technology Environment**

- Focuses on auditing IT systems, controls, and cybersecurity measures.
- Highlights the importance of data integrity, privacy, and system reliability.

- Recommends staying updated on evolving technology risks.

➤ **SIA 530: Third Party Service Provider**

- Guides auditors on assessing risks associated with outsourcing.
- Emphasizes evaluating third-party compliance and performance.
- Focuses on ensuring contract terms align with organizational goals.

■ **Standards Issued up to July 1, 2013**

➤ **SIA 5: Sampling**

- Explains methodologies for selecting representative samples.
- Emphasizes accuracy and reliability in sample-based audits.
- Recommends statistical and non-statistical sampling techniques.

➤ **SIA 6: Analytical Procedures**

- Guides auditors on using analytics to identify trends and anomalies.
- Recommends integrating data analysis in risk-based audits.
- Focuses on cost-effective and efficient audit practices.

➤ **SIA 7: Quality Assurance in Internal Audit**

- Highlights the importance of quality parameters in audits.
- Recommends periodic reviews and adherence to professional standards.

- Encourages continuous improvement through feedback and training.

**SIA 11: Consideration of Fraud in an Internal Audit**

- Provides a framework for identifying potential fraud risks.
- Recommends proactive measures to detect and mitigate fraud.
- Focuses on ensuring ethical practices within the organization.

**SIA 18: Related Parties**

- Guides auditors on identifying and auditing related-party transactions.
- Emphasizes transparency and compliance with disclosure requirements.
- Recommends ensuring fairness and preventing conflicts of interest.

3.1. Company Law Regulation

The Companies Act, 2013 has been a watershed milestone in the corporate governance and formal recognition of the function of internal audit. The Act and the Rules framed thereunder have introduced provisions relating to mandatory requirement of internal audit for mid sized and large companies, the role of internal auditors, Board of Directors, Audit Committee, and top Management.

As per Section 138 of the Companies Act, 2013, the following categories of companies are mandatorily required to appoint an internal auditor:

Parameters of internal audit applicability	Unlisted Company (Amount in Rs. Crore)		Listed Company
	Public Company	Private Company	
Turnover	200	200	Fully applicable irrespective of any of the parameters
Loans or borrowings	100	100	
Paid up share capital	50	Not Applicable	
Deposits	25	Not Applicable	

- **Due date for appointment of an Internal Auditor:** An existing company covered under any of the above criteria shall appoint an Internal Auditor within 6 months.

■ **Who can be an Internal Auditor?**

The following can be appointed as an Internal Auditor:

- a chartered accountant, or
- a cost accountant, or
- Such other professional as may be decided by the Board.

The Audit Committee or Board of the company shall, in consultation with the Internal Auditor, formulate the scope, functioning, periodicity and methodology for conducting the internal audit.

- The **internal auditor** responsibilities include:

- Assessing internal controls and compliance with applicable laws and regulations to the company.
- Conducting audits to ensure the Company is in compliance with internal policies and external regulations.
- Ensuring that the internal audit system aligns with the company's operational needs and regulatory requirements.
- Collaborating with the audit committee to define the scope and methodology of audits
- Reporting directly to the audit committee or board of directors.
- Evaluation of internal financial controls and risk management systems;
- Conducting an independent assessment and evaluation of control systems throughout the organization, including both financial controls and operational areas, to identify potential opportunities for improvement.
- Determining the degree of adherence to established policies, procedures, regulations, and applicable legislation.
- Checking compliance management systems of an organization.
- Promote effective risk management practices by implementing systems to identify, assess, manage, and, where feasible, mitigate or distribute risks.
- Drive cost savings by pinpointing areas of waste, inefficiency, and duplication of efforts across the organization.
- Design programs and activities to protect company assets, incorporating internal control mechanisms to minimize fraud risks and establish early warning systems for detecting potential fraud.

■ The **Audit Committee** shall perform the following role:

- review and monitor the auditor's independence and performance, and

effectiveness of audit process;

- carry out evaluation of internal financial controls and risk management systems;
- obtain feedback and comments of the internal auditors about internal control systems, the scope of audit, including the observations of the auditors and review of financial statement before their submission to the Board

■ The **Board of Directors** shall perform the following role:

- Appointing internal auditors based on recommendations from the audit committee.
- Ensuring that adequate resources are allocated for effective internal audit functions.
- Reviewing reports from both internal and external auditors to maintain oversight on company operations auditor.

3.2. Implementation of Other Frameworks

The provisions of the Companies Act, 2013 have made the Board of the companies responsible for ensuring that following frameworks are put in place, monitored regularly and reported upon, as a part of overall corporate governance. The Board's responsibilities include:

Internal Financial Controls (IFC)	Enterprise Risk Management System (ERM)	Fraud Risk Management (FRM)	Legal Compliance Framework (LCF)
<ul style="list-style-type: none">● Policies and procedures to ensure efficient conduct of business– Safeguarding	<ul style="list-style-type: none">● Approving and monitoring the ERM● ERM includes:	<ul style="list-style-type: none">● Preventing and detecting Frauds● FRM includes<ul style="list-style-type: none">– Creating control	<ul style="list-style-type: none">● Devising proper systems to ensure compliance to applicable

Internal Financial Controls (IFC)	Enterprise Risk Management System (ERM)	Fraud Risk Management (FRM)	Legal Compliance Framework (LCF)
<div>of assets</div> <ul style="list-style-type: none">– Prevention and detection of frauds and errors– Accuracy and completeness of accounting records– Timely preparation of reliable financial information.	<ul style="list-style-type: none">– Identification of significant risk exposures– Assessing the impact of significant risk exposures– Action plan for risk mitigation– Monitoring progress	<div>environment</div> <ul style="list-style-type: none">– Conduct of fraud risk assessment– Establishing prevention techniques to avoid key risk– Promoting tools for reporting suspicious activities– Response to fraud allegation	<div>laws</div> <ul style="list-style-type: none">● LCF includes– Identification of all applicable laws and their requirements– Development of system to ensure compliance– Ensuring training and awareness among employees– Monitoring compliance status

The above requirements have also widened the roles and responsibilities of the internal audit function as to ensure that such frameworks are designed and implemented by the companies, verifying the existence and effectiveness of these frameworks, appropriate reporting, etc.

3.3. Other Important Regulatory Aspects

3.3.1. Serious Fraud Investigation Office (SFIO)

The Government of India had set up a committee on corporate governance under the chairmanship of Shri Naresh Chandra, former Cabinet Secretary. The Naresh Chandra Committee inter-alia recommended setting up of Corporate Serious Fraud Office.

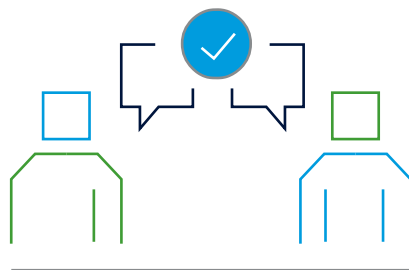
As per the Companies Act, 2013, SFIO has been established through the Government of India vide Notification NO. S.O.2005 (E) dated 21 July 2015. It is a multi-disciplinary organisation under the Ministry of Corporate Affairs, consisting of experts in the field of accountancy, forensic auditing, banking, law, information technology, investigation, company law, capital market and taxation etc. for detecting and prosecuting or recommending for prosecution white collar crimes/ frauds.

Investigation into the affairs of a company is assigned to SFIO, where Government is of the opinion that it is necessary to investigate into the affairs of a company:

- a. on receipt of a report of the Registrar or inspector under section 208 of the Companies Act, 2013;
- b. on intimation of a special resolution passed by a company that its affairs are required to be investigated;
- c. in the public interest; or
- d. on request from any department of the Central Government or a State Government

3.3.2. Establishment of Vigil Mechanism

Whistle blowing means inviting the attention of the top management to wrongdoings and frauds occurring within an organisation. The term is now being heard more than ever before, as the media, corporates and the public are now becoming increasingly aware of the concept, but unfortunately until the New Companies Act, 2013, there were no safeguards provided to a whistle blower.



All the listed companies or companies which accept deposits from the public or companies which have borrowed money from banks and Public Financial

Institutions (PFIs) in excess of Rs. 50 crores under section 177(9) read with Companies (Meetings of Board and its Powers) Rules, 2014, are required to establish a vigil mechanism for directors and employees to report genuine concerns in such manner as may be prescribed. The details of establishment of such mechanism shall be disclosed by the company on its website, if any, and in the Board's report. The vigil mechanism should also provide for adequate safeguards against victimisation of persons who use such mechanism and make provision for direct access to the chairperson of the Audit Committee in appropriate or exceptional cases.

In case of repeated frivolous complaints being filed by a director or an employee, the audit committee or the director nominated to play the role of audit committee may take suitable action against the concerned director or employee, including reprimand.

3.3.3. Introduction of provisions relating to frauds

The Central Government seeks the support of auditors in bringing transparency and discipline in the corporate world to protect the interests of the shareholders and public at large. Hence, the Companies Act, 2013 has come up with more specific and clear provisions relating to fraud & fraud reporting.

The Fraud provisions are in force with effect from 12 September 2013 and the Fraud reporting provisions are brought in force with effect from 1 April 2014 and were amended by the Companies Amendment Act, 2015. On 14 December 2015, the Ministry of Corporate Affairs (MCA) issued a notification pertaining to reporting of frauds (Rule 13 to the Companies (Audit and Auditors) Amendment Rules, 2015) specifying threshold value of fraud loss from a reporting standpoint. The notification states that if an auditor has "reason to believe" that fraud, which involves or could potentially involve individually an amount of rupees one crore or above, is being or has been committed against the company, the auditor needs to report the matter to the Central Government within 60 days of his or her knowledge of such a fraud. The process for doing this, includes reporting the matter to the company's Board or the Audit Committee within 2 days (of coming

to know about the fraud), seeking a response from the Board or Audit Committee on the matter (within 45 days), and forwarding this response along with the auditor's own report to the Central Government (within 15 days). In case of no response from the Board or Audit Committee, the auditor's report along with the communication sent to the Board should be forwarded to the Central Government. In case of a fraud involving amounts less than rupees one crore, the auditor needs to report the matter to the Audit Committee or the Board within 2 days of coming to know about the fraud. The MCA requires each of such frauds to be disclosed in the Board's Report. Contents of the auditor's report should include nature of the fraud and a brief description, approximate amount involved in the fraud and potential parties involved. Additionally, the Board's Report should also mention 'Remedial actions taken' in that regard.

The new Act has specifically provided a stringent punishment with respect to fraud. Under section 447 of the Companies Act, 2013, any person who is found to be guilty of fraud, shall be punishable with imprisonment for a term which shall not be less than six months but which may extend to ten years and shall also be liable to fine which shall not be less than the amount involved in the fraud, but which may extend to three times the amount involved in the fraud.

The Director, Additional Director or Assistant Director of the SFIO on the basis of material in his possession can arrest any person in case he has reason to believe (the reason for such belief to be recorded in writing) that the person is guilty of an offence of corporate fraud covered under Section 447 of the Act. In case of foreign companies and government companies, prior written approval of the Central Government for arrest would be required. The SFIO is required to maintain an arrest register with relevant details of the arrestee, the date and time of arrest, and various other particulars. The provisions of the Code of Criminal procedure, 1973 relating to arrest shall be applicable.

3.3.4. Class Action suits

On 1 June 2016, the Ministry of Corporate Affairs, notified section 245 of the Companies Act, 2013, enlisting the provisions of class action suits in India. In a class

action suit, the shareholders of a company collectively institute a suit against the company.

The requirement for provisions of class action suits in India was primarily triggered by the Satyam scam. Satyam shareholders were unsuccessful in claiming damages in India due to the absence of the provision for filing a class action suit under the Companies Act, 1956. On the other hand, the American investors were able to claim their part of damages in the US courts through a class action suit against the company. Accordingly, provisions of class action suit were incorporated to safeguard the interests of shareholders, whenever the company or its directors participate in any fraudulent, unlawful act, or commit an act which is against the interest of the shareholders. The members or the depositors can seek damages or demand suitable action against a director, auditor, expert, advisor or consultant of the company.

In light of the above developments emphasising the need of robust Corporate Governance, the Internal Audit function is expected to cover these areas in the internal audit scope depending on the risk-based audit plan.

3.4. RBI Regulations

A. Regulatory Overview – Risk Based Internal Audit in Banks

The **Reserve Bank of India** has provided guidelines for **Risk Based Internal Audit in Banks** and **NBFCs** through following circulars:

	Circular / Guidelines	Reference	Date of the Circular / Guidelines
1	Risk-based internal audit – Banks	DBS.CO.PP.BC . 10 /11.01.005/2002-03	December 27, 2002
2	Risk-based internal audit – Guidance Note–Banks	DBS.CO.PP.BC . 10 /11.01.005/2002-03	December 27, 2002
3	Risk Based Internal Audit (RBIA) Framework – Strengthening Governance arrangements– Banks	RBI/2020-21/83 Ref.No.DoS.CO.PPG./	January 07, 2021

	Circular / Guidelines	Reference	Date of the Circular / Guidelines
4	Risk-based internal audit – NBFCs	RBI/2020-21/88 Ref.No.DoS.CO.PPG./	February 03, 2021

3.4.1. Background:

The circulars set out the basic approach for risk based internal audit functions, aligned with prevailing best practices as part of the overall Governance and Internal Control framework. The objective of the approach is to build a strong internal control framework to keep pace with the complexities that Indian banks are exposed to as a result of the evolution of financial instruments and markets , subsequent to the liberalisation of the Indian financial sector. A robust internal audit function is perceived as a key component for the effectiveness of the internal control system. Hitherto, internal auditors focussed efforts on testing of accuracy and reliability of accounting records and financial reports, integrity, reliability and timeliness of control reports, compliance to legal and regulatory requirements and testing of transactions. In view of the changing scenario, the internal audit function is envisaged as one that evaluated and performed an independent risk assessment of all activities of the bank including the risk management function.

The Key requirements/ components for Banks include:

■ **Policy for risk-based internal audit**

The guidance note prescribes a risk-based assessment of various areas and prioritization of areas for audit and allocation of resources based on risk assessment. This would require to be documented in a Board approved Risk based Internal Audit Policy which defined the risk assessment methodology including the period within which low risk area were to be subjected to audit.

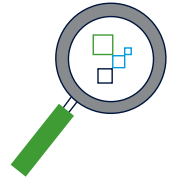
■ **Functional independence of the Internal Audit Department:**

The guidance note also prescribes the independence of the Internal Audit function from the internal control process in order to maintain

independence. Ordinarily, the function would have a reporting line to the Board of Directors / Audit Committee of the Board. It places responsibility for having an effective risk-based internal audit system on the Board and top management.

➤ **Risk assessment**

The risk assessment process would include building up a risk matrix after considering the inherent business risks and evaluation of the internal controls or control risks associated to classify the risks as High, Medium or Low. The basis for determining the risk should be clearly explained. The guidance also prescribed spelling out a decreasing, stable or increasing trend of business and control risks. The risk assessment methodology should consider impact of internal and external environment including internal audit reports and compliance, changes in lines of business, change in management / key personnel, results of regulatory examinations and external auditors' reports, business volumes and complexities and industry trends amongst others



➤ **Audit Plan:**

The audit plan should be approved by the board and define the frequency of the audit. The higher risk areas should be audited more frequently than the lower risk areas and the plan should provide a rationale for the audit work to be performed. Regulatory guidelines and requirements would also have a bearing on the frequency of the audits.

➤ **Scope**

The scope should be designed in a manner that reasonable assurance to the Board and top management on the adequacy and effectiveness of the risk management and control framework.

Transaction testing would form an important part of the audit scope and the risk ratings of the areas and the direction of risk would dictate the extent of testing. The scope should also include recommending corrective measures and undertaking follow up reviews to track the actions taken per the action plans. The scope should include process by which risks are identified and managed in various areas, the control environment in various areas, gaps, if any, in control mechanism which might lead to frauds, identification of fraud prone areas, data integrity, reliability and integrity of MIS, internal, regulatory and statutory compliance, budgetary control and performance reviews, monitoring compliance with the risk-based internal audit report and variations, if any, in the assessment of risks under the audit plan.



Communication

The communication channels should encourage reporting and highlighting of deficiencies in controls and sensitive or negative findings at appropriate levels of management as and when these are identified. This includes flagging off significant risks to the Board and Audit Committee.



Performance reviews

The Internal Audit Department should conduct reviews at predefined intervals (annually or more frequently) of the internal audit undertaken against the approved audit plan. The performance review should evaluate the effectiveness of the audits in mitigating identified risks. The Board of Directors/ Audit Committee of Board should similarly perform effectiveness assessments of reasonableness of risk assessment methodology of the Internal Audit Department.



Resources

The Internal Audit department should be provided adequate and skilled resources to carry out the risk based internal audits. Internal Audit department should organise periodic trainings for the staff related to bank's business, operating procedures, risk management and control systems etc.

In addition to the basic approach for risk based internal audit functions, defined in the Guidance Note of December 2002, the RBI Circular of January 7, 2021 advises the banks to align to evolving business practices as under:

- **Authority, Stature and Independence:**

Head of Internal Audit (HIA) shall be a senior executive of the bank with the ability to exercise independent judgement. In order to carry out the activities objectively the department must have the required authority, independence, stature and access to records and personnel in the bank at all times. Moreover, the department should be adequately staffed.

- **Competence:**

In order to carry out audit effectively the staff should have the requisite knowledge, competence and experience in banking operations, accounting, information technology, data analytics and forensic investigation, amongst others

- **Staff Rotation:**

Other than instances where the internal audit function is managed by career audit staff, the Board and senior management should prescribe a minimum period of review for staff in the Internal Audit department. In case of staff who possess specialized skills, the Board should prescribe a

minimum stint with the Internal Audit department, to facilitate building of those skills in the Internal Audit Department.

- **Tenor of the Head of Internal Audit (HIA):**

The HIA shall be appointed for a minimum of three years except for banks which have a specialised function and managed by career internal auditors.

- **Reporting Line:**

The HIA shall directly report to either the Audit Committee of the Board (ACB) / MD & CEO or Whole Time Director (WTD). In case the Board allows the HIA to report to e MD & CEO or a WTD, the ACB shall be 'reviewing authority' and the Board shall be 'accepting authority' in case of the performance appraisal of the HIA. Additionally, the ACB shall meet the HIA, at least, once every quarter, without the presence of the senior management, including the MD & CEO/WTD. The HIA will also not have any business targets any reporting responsibility to any of the business heads. In the context of the foreign banks operating as branches in India, the HIA's reporting shall be to the internal audit function in the controlling office / head office.

- **Remuneration:**

To avoid conflict of interest and ensure the auditor's independence and objectivity, the audit staff's remuneration shall not be linked to the financial performance or results of the business verticals.

Outsourcing of the internal audit function is not permitted. Experts, including former employees, may be hired on a contractual basis, if expertise in the required area of audit

does not reside within the bank's Internal Audit function. The ACB should be assured in this regard and conflict, if any, arising out of such an arrangement should be addressed. The bank's internal audit function shall have the ownership related to the audit reports.

B. Regulatory Overview – Risk Based Internal Audit in NBFCs

The RBI further mandated the applicability of the RBIA framework for the following Non-Banking Financial Companies (NBFCs) and Primary (Urban) Co-operative Banks (UCBs) vide circular 3 February 2021 to:

- a. All deposit taking NBFCs, irrespective of their size;
- b. All Non-deposit taking NBFCs (including Core Investment Companies) with asset size of 5,000 crore and above; and
- c. All UCBs having asset size of 500 crore and above

The circular mandated the implementation of the requirements to the above mentioned entities by March 31, 2022. The objectives of the circular are as under:

- An effective Risk-Based Internal Audit (RBIA) is an audit methodology that links an organisation's overall risk management framework and provides an assurance to the Board of Directors and the Senior Management on the quality and effectiveness of the organisation's internal controls, risk management and governance related systems and processes.
- The internal audit function should broadly assess and contribute to the overall improvement of the organization's governance, risk management, and control processes using a systematic and disciplined approach. The function is an integral part of sound corporate governance and is considered as the third line of defence.

- Historically, the internal audit system in NBFCs/UCBs has generally been concentrating on transaction testing, testing of accuracy and reliability of accounting records and financial reports, adherence to legal and regulatory requirements, etc. However, in the changing scenario, such testing by itself might not be sufficient. Therefore, SEs will have to move towards a framework which will include, in addition to selective transaction testing, an evaluation of the risk management systems and control procedures in various areas of operations. This will also help in anticipating areas of potential risks and mitigating such risks.
- While the Risk Management Function should focus on identification, measurement, monitoring, and management of risks, development of risk policies and procedures, use of risk management models, etc., RBIA should undertake an independent risk assessment for the purpose of formulating a risk-based audit plan which considers the inherent business risks emanating from an activity / location and the effectiveness of the control systems for monitoring such inherent risks.

The key roles and responsibilities of the various functionaries in the context of the Internal Audit function are as under:

■ **Board of Directors / Audit Committee of Board**

The primary responsibility for oversight of the internal audit function rests with the Board of Directors (the Board) / Audit Committee of Board (ACB) of NBFCs and the Board of UCBs. The Board approved RBIA policy should be disseminated within the organization and subject to periodic review. The policy shall set out the purpose, authority, and responsibility of the internal audit activity, clearly demarcating the role and expectations from Risk Management Function and Risk Based Internal Audit Function. The policy should be aligned with the size, complexity and nature of the business.

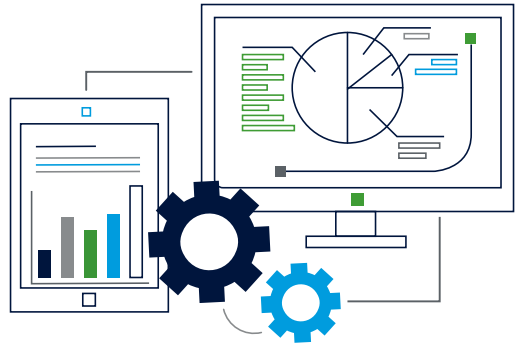
It should take into account aspects related to the independence, objectivity, professional ethics, accountability of the internal audit department. The ACB/Board shall approve a RBIA plan whose priorities should be aligned to the overall goals and objectives of the organisation. The risk assessment should be performed on an annual basis and should cover every location and the risk management and compliance functions. The plan should specify the maximum period within which the low risk areas should be audited. The Board/ ACB should formulate and maintain a quality assurance and improvement program that covers all aspects of the internal audit function. The quality assurance program should perform the review the Internal Audit function at least once in a year for adherence to the internal audit policy, objectives and expected outcomes. The Board/ ACB may promote the use of tools and techniques to perform the actual review.

■ **Senior Management**

The senior management is responsible for ensuring adherence to the internal audit policy guidelines and building an effective internal control function for identification, measurement, monitoring and reporting of all risks. They are also responsible for timely implementation of the action plans of audit issues and providing status updates on the closure. They are also responsible for establishing a comprehensive and independent internal audit function. The function should be adequately staffed with skilled personnel who should be trained periodically. They are also responsible for promoting transparency and accountability. They are also responsible for providing a consolidated position on all risks that the entity faces at least on an annual basis to the Board/ ACB including inputs from Internal and other auditor.

The significance of the Internal Audit (IA) function is evident from the discussions in this publication. IA can bring value by objectively evaluating risks, assessing processes and systems for efficiencies and meeting business objectives. Internal Audit should be a valued business partner to the organisation.

The Internal Audit (IA) function is the Third Line of Defence which oversees the risks and controls within the operations of an organization and also helps safeguarding Corporate Governance framework.



Internal audits can aid organisations by:

- Evaluating risk management, governance, and control processes
- Ensuring internal controls are adequate and effective
- Assessing ethics, economy and efficiency across organisation
- Communicating information and opinions clearly and accurately

With the global economy facing challenges and uncertainties, the key stakeholders of organizations are seeking an approach to IA that goes beyond reviewing past activities. They want an IA function that is insightful, forward-looking, and which is not afraid to go beyond preserving current assets, instead focuses on creating value on a departmental, divisional, or organizational level.

One of the features that makes internal auditing so valuable to modern enterprises is that it serves multiple stakeholders, including the board, various levels of management, and even external auditors and regulators.

The major stakeholders of internal audit are:

Though the prime expectation from the IA function is about providing an independent assurance on the organizational effectiveness of risk management, governance and internal controls and processes, the expectations of the Board and other stakeholders from the IA function have increased multi fold over the years.

The Internal Audit should adopt technology and strive to innovate in meeting and exceeding stakeholders' expectations. There are situations where multiple stakeholders have different expectations and trying to satisfy everyone can become particularly problematic if the disagreement is between the audit committee and management. In such cases, the IA is usually caught between powerful forces and have to walk a very tight rope keeping in mind the broad

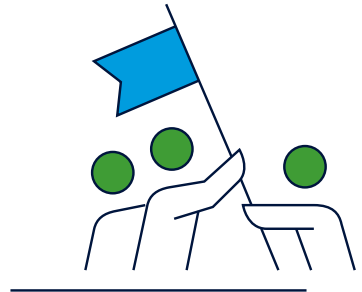
objectives of IA and its alignment to the organizational goals.

4.1 Key Stakeholders' Expectations from IA

In the modern world order of geo-political and economic uncertainties, market volatility, dynamic business environment, technological and digital disruptions, frauds, cyber threats, increased regulatory compliances, investor demands for greater transparency, etc. have all significantly heightened and expanded the expectations from IA.

The varied groups of stakeholders as mentioned above have different expectations, some of the important and common expectations are:

4.1.1 Paradigm shift in role of IA – the IA role has moved from hindsight to insight and finally towards foresight. The Board expects an objective and independent assurance and critical insights to operations to support management decision making.



4.1.2 Aligning organization's objectives – The IA function must strategically align its objectives with the broader organizational goals to maintain relevance and effectiveness. By integrating with the company's strategic vision, IA can pinpoint and address potential risks that might impede achieving these goals. This necessitates a comprehensive understanding of the organization's strategic objectives, business model, and key performance indicators (KPIs).

4.1.3 Assurance on Risk Management – assess effectiveness of risk management by recommending improvement measures to strengthen risk framework and advice in risk monitoring. With combination of assessing risk horizon with business knowledge, it should provide a continuous assurance on the effectiveness of the risk design. This includes evaluating the effectiveness of the risk assessment process and the quality of the risk management plans that are put in place to address identified risks.

4.1.4 Internal controls framework – highlighting any weaknesses or deficiencies in design of internal controls framework to ensure that controls are effectively implemented and timely monitored.

4.1.5 Use of Technology and techniques – to enhance productivity and ensure that risks associated with technology are addressed effectively. In today's unpredictable environment, organizations must be prepared for various crises, including natural disasters, cyber-attacks, and pandemics. IA can add value by assessing the effectiveness of existing crisis management plans, recommending improvements, and ensuring the organization is well-prepared to respond to and recover from potential crises.

The potential for making value through technology is enormous, especially if IA is able to integrate a higher level of data analytics into its audit approach. An integrated approach to using Data Analytics throughout the audit process (for example, analytics-driven continuous auditing, dynamic audit planning, audit scoping and planning, audit execution and reporting) would provide greater insights and value.

Effective examples of IA in action include integrating machine learning algorithms to enhance predictive auditing or collaborating with cybersecurity teams to strengthen the organization's defences against cyber threats.

4.1.6 Provide insight into global best practices – highlighting key processes within the organization that require improvement based on industry benchmarks.

4.1.7 Partner in progress and be a value creator – Explore cost savings and optimisation opportunities

4.1.8 Subject Matter Expertise – in the modern days, IA is expected to horn and acquire newer skills, beyond the accounting and financials fields. The IA team needs to include experts from multi-disciplinary streams. Since the role of IA has shifted to also review operations of the organisations, it is expected to review technical areas of operations to provide its independent and fair view of the operations and also suggest measure to improve efficiencies.

- 4.1.9 Support greater compliance** – in today's era of complex and challenging legal environment, IA can support better compliance with laws and regulations, internal processes and practices, guide the management towards achieving a higher level of compliance.
- 4.1.10 Provide effective Solutions** – IA should focus on "How to solve the problems and not just to point out the problems". IA should provide specific, measurable, achievable, realistic and time bound (SMART) recommendations that address the root cause accurately and in a more meaningful manner.
- 4.1.11 Foster continuous improvements & Learnings** – IA must stay abreast of the latest developments in auditing, risk management, and corporate governance. Investing in ongoing training and professional development for the IA team is vital. This ensures that the team possesses the skills and knowledge required to address emerging risks and leverage advanced technologies effectively.
- 4.1.12 Effective coordination among assurance functions** – a stronger alignment of IA with other assurance functions within the organization, as for example Compliance, Legal or Risk Management, external auditors, etc. is needed when it comes down to developing the strategic audit plan and preparing the scope of specific audits.
- 4.1.13 Continuous monitoring** – these days organisations demand continuous monitoring of operations rather than periodic reviews to ensure that any unfavourable incidences are captured and assessed well in time before it causes any damages so that effective solutions can be implemented. The IA is expected to play vital role in continuous reviews of organisations processes, practices and operations.
- 4.1.14 Maintaining independence and objectivity** – IA can provide unbiased insights and recommendations while being recognized as a valuable partner in the organization's success. While remaining independent from the organization and by not taking on managerial ownership for managing risk, IA should seek to get more preliminary insights and intelligence from the other risk tracking and facilitating

functions. This would allow the stakeholders to have a more comprehensive, overall view on the corporate governance state of the organization and to understand if key risks are adequately addressed in terms of monitoring and auditing.

4.1.15 Ethical considerations and corporate social responsibility (CSR) – IA should ensure that the organization adheres to high ethical standards and complies with CSR commitments. This involves regular assessments of the organization's ethical practices, sustainability initiatives, and social impact, providing recommendations for improvement where necessary. For example, IA can evaluate the effectiveness of the company's environmental sustainability programs and suggest enhancements to reduce its carbon footprint.

4.1.16 Effective Communication – Transparent and regular updates on audit findings, risk assessments, and recommendations are essential. IA should ensure that its reports are not only comprehensive and accurate but also presented clearly and understandably for all stakeholders. This transparency helps build trust and confidence in the IA function. Ensure audit reports and presentations are clear, succinct, impactful and delivered on a timely basis.

4.1.17 Fraud Detection and Prevention – With the rising incidence of fraud and corruption globally, stakeholders expect IA to play a proactive role in identifying potential fraud risks and implementing robust controls to mitigate them. Utilizing advanced data analytics and forensic techniques to detect anomalies and irregularities that may indicate fraudulent activities is essential.

4.2 Necessity of Internal Auditor to meet the Audit Committee of the Board

Internal Auditor does not have to wait for the quarterly/scheduled meetings to reach out to the Audit Committee if critical trigger events or urgent issues arise. The Internal Auditor is empowered to communicate significant risks or findings to the Audit Committee immediately, especially if the situation requires prompt attention to safeguard the organization.

Protocol for Reaching Out:

- **Prompt Notification:** The Internal Auditor should directly notify the Audit Committee Chair, either in writing or via a private discussion, regarding the critical issue.
- **Confidential Handling:** Maintain confidentiality, particularly in matters involving fraud, whistleblowers, or sensitive ethical concerns.
- **Requesting Special Meetings:** The Internal Auditor may request a special meeting of the Audit Committee or Board to address the issue if it cannot wait until the next scheduled meeting.



These steps align with professional responsibilities and the Internal Auditor's duty to act as an independent and objective assurance provider to the organization.

The Internal Auditor may request a private session with the Audit Committee and Board to alert them about critical issues under the following trigger events:

- **Significant Control Failures**

Identification of critical weaknesses or notable deficiencies in internal controls that could compromise the organization's financial reporting, operational effectiveness, or compliance processes.

- **Fraud or Misconduct**

Indications of fraudulent activities, unethical behaviour, or illegal actions by senior management or key personnel that could result in reputational damage or financial loss for the organization.

- **Conflicts of Interest**

Identification of significant conflicts of interest, especially those involving

senior executives or board members, that compromise decision-making or governance.

■ **Risk of Material Misstatements**

Identification of risks that could result in material misstatements in the financial statements, impacting investor confidence or compliance with reporting standards.

Concerns over the organization's financial stability, liquidity position, or ability to continue as a going concern.

■ **Breakdown of Governance Processes**

Failures or inefficiencies in governance frameworks, manifested through lack of accountability, subpar decision-making, or insufficient oversight.

■ **Cybersecurity Threats or Breaches**

Cybersecurity incidents, data breaches, or exploitable vulnerabilities that could expose the organization to reputational damage, regulatory scrutiny, or substantial financial loss.

■ **Management Override of Controls**

Identified instances of senior management overriding established internal controls for personal gain or to achieve short-term objectives.

■ **Whistleblower Complaints**

Verified whistleblower allegations revealing significant misconduct or systemic issues within the organization.

■ **Critical Audit Findings Ignored**

Instances where prior internal audit findings or recommendations have been ignored or inadequately addressed by management, potentially escalating risks.

- **Confidential Matters**

Sensitive or confidential matters that are unsuitable for open discussion but require the attention of the Audit Committee or Board.

- **Ethical or Reputational Risks**

Any matter that could substantially harm the organization's reputation, brand, or ethical standing in the public eye.

- **Role of the Internal Auditor:** It is the responsibility of the Internal Auditor to act independently and provide an unbiased view of the identified risks on a timely manner.

To conclude, the IA function has to continuously assess its to ensure that the collective expectations of all relevant stakeholders are balanced and met with, if not exceeded.

Chapter 5 Role of Subject Matter Experts in enhancing value proposition of Internal Audit

Internal Audit plays a pivotal role in safeguarding an organization's assets, ensuring compliance with regulations, and improving operational efficiency. While internal auditors possess a comprehensive understanding of audit methodologies and best practices, their effectiveness can be significantly enhanced by the strategic involvement of Subject Matter Experts (SMEs).

5.1 Defining a Subject Matter Expert (SME)

An SME is an expert with specialised knowledge in a particular segment or a knowledge domain. This expertise is typically acquired through a combination of education, training, and years of practical experience. In the context of internal audits, SMEs can be drawn from various sources, including:

- **Internal Employees:** Individuals within the organization with in-depth knowledge of specific processes, systems, or departments.
- **External Consultants:** Industry professionals with specialized expertise in areas such as cybersecurity, regulatory compliance, or fraud risk management.
- **Industry Experts:** Academics, researchers, or professionals from other organizations with a deep understanding of industry-specific challenges and best practices

In essence, a subject matter expert is a go-to person for information, guidance, and expertise in a particular field. Their knowledge and experience are invaluable assets in a wide range of settings.

It may be pertinent to note that by not involving Subject Matter Experts (SMEs) in internal audits can lead to several significant challenges:

- **Incomplete Risk Assessment:** Without the insights of SMEs, internal auditors may not fully understand the organization's unique risks and control environment. This can lead to incomplete or inaccurate risk assessments, potentially missing critical areas of concern.

- **Inefficient Audit Planning:** SMEs can provide valuable information on the organization's processes, systems, and controls.¹ Without this input, audit planning may be less efficient, leading to wasted time and resources on areas of low risk or overlooking high-risk areas.
- **Limited Audit Scope:** SMEs can help identify areas of significant risk and complexity that require more in-depth examination. Without their input, the audit scope may be too narrow, failing to address critical issues.
- **Difficulty Interpreting Findings:** Internal auditors may have a limited understanding of the context and implications of their audit findings. SMEs can help interpret these findings, ensuring that they are accurately understood and communicated to management.
- **Less Effective Recommendations:** Without the expertise of SMEs, recommendations for improvement may be less relevant, practical, or effective. SMEs can provide valuable insights on the feasibility and practicality of different solutions.
- **Reduced Audit Quality:** Overall, the absence of SME involvement can lead to a reduction in the quality of internal audits. This can result in a higher risk of undetected errors, fraud, or non-compliance.

5.2 Enhancing Role of Internal Audit by Involving Subject Matter Experts:

The role of internal audit is evolving to meet the needs of a complex and ever-changing business landscape. Engaging subject matter experts (SMEs) is a key strategy to elevate internal audit's value and impact.

5.2.1 Importance of Internal Audit in Today's Business Environment:

- **Risk Assessment:** Internal audit helps organizations identify, assess, and manage various business risks, enabling proactive risk mitigation.
- **Compliance & Governance:** Internal audit ensures compliance with relevant regulations and standards, promoting ethical conduct and good governance.

- **Process Efficiency:** Internal audit reviews business processes, identifying opportunities for improvement and optimization to enhance efficiency.

The involvement of Subject Matter Experts can significantly enhance internal audit capabilities through.

5.2.2 Enhanced Technical Depth:

SMEs bring specialized knowledge that enables more thorough evaluation of complex processes, systems, and controls. Their expertise allows for:

- More accurate risk assessment in specialized areas
- Better understanding of technical complexities
- More precise audit findings and recommendations

5.2.3 Improved Stakeholder Confidence:

The involvement of recognized experts increases stakeholder trust in audit findings and recommendations, particularly in specialized or technical areas.

5.2.4 Knowledge Transfer:

SMEs can help build internal audit team capabilities through:

- Training and mentoring
- Development of specialized audit programs
- Creation of technical guidance materials

5.3 Integrating Subject Matter Experts into the Audit Process:

5.3.1 Planning Phase:

The involvement of Subject Matter Experts (SMEs) during the planning phase of an internal audit can significantly enhance its effectiveness and efficiency. Here's how:

■ **Risk Identification and Prioritization:**

- **In-depth Industry Knowledge:** SMEs possess a deep understanding of industry-specific risks, regulations, and best practices. This knowledge allows them to identify potential risks that internal auditors might overlook, leading to a more comprehensive risk assessment.
- **Process Expertise:** SMEs can provide valuable insights into the organization's processes, systems, and controls. This knowledge helps prioritize audit areas based on their criticality and the associated level of risk.

■ **Scope Definition and Resource Allocation:**

- **Tailored Approach:** SMEs can help tailor the audit scope to the specific needs and circumstances of the organization. This ensures that the audit focuses on the most critical areas and avoids wasting resources on areas of low risk.
- **Efficient Resource Utilization:** By providing insights into the complexity and resource requirements of different areas, SMEs can help optimize the allocation of audit resources, ensuring efficient and effective use of time and personnel.

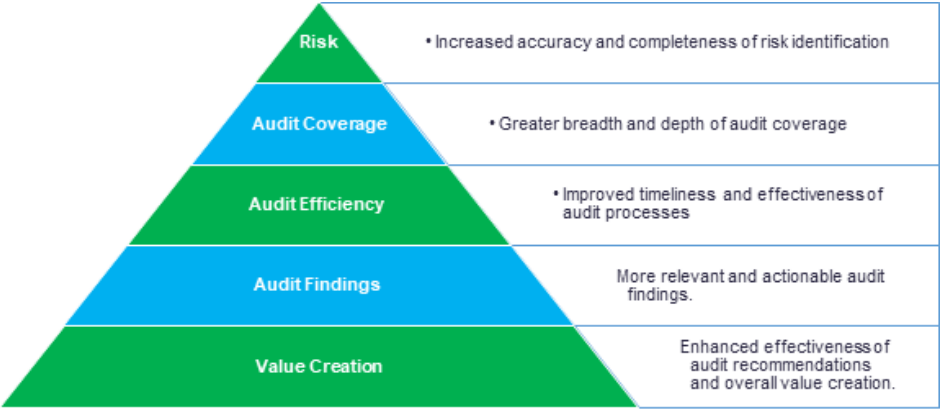
■ **Improved Communication and Collaboration:**

- **Stakeholder Buy-in:** Involving SMEs in the planning phase can increase stakeholder buy-in and support for the audit process. This can facilitate smoother audit execution and improve the overall effectiveness of the audit.
- **Enhanced Communication:** SMEs can act as a bridge between the audit team and the business units, facilitating clear communication and understanding of audit objectives and expectations.

- **Early Identification of Potential Issues:**
 - **Proactive Approach:** By involving SMEs early in the planning phase, potential issues and challenges can be identified and addressed proactively. This can save time and resources during the actual audit execution.
- **Increased Audit Relevance:**
 - **Business Context:** SMEs can provide valuable context for the audit, ensuring that the audit findings are relevant and meaningful to the business. This can lead to more actionable recommendations and a greater impact on the organization's risk management and control environment.

In summary, the involvement of SMEs in the planning phase of an internal audit is crucial for ensuring that the audit is effective, efficient, and aligned with the organization's specific needs and objectives. By leveraging the expertise of SMEs, organizations can enhance the value and impact of their internal audit function.

Depiction of how SME involvement brings value addition to Internal Audit



5.3.2 Execution Phase

SMEs contribute to data gathering, risk assessment, and control evaluation by providing expert insights.

During the execution phase of an internal audit, Subject Matter Experts (SMEs) play a vital role in enhancing the quality and effectiveness of the audit process. Here are some keyways they contribute:

- **Providing Technical Expertise:**
 - **Complex Areas:** SMEs can provide in-depth knowledge and guidance on complex technical areas that may be beyond the expertise of the internal audit team. This ensures that the audit procedures are appropriate and effective in assessing the relevant controls.
 - **Data Interpretation:** SMEs can help interpret technical data, such as system logs, production data, or financial reports, and identify potential anomalies or areas of concern.
- **Enhancing Audit Procedures:**
 - **Identifying Control Gaps:** SMEs can help identify potential control gaps or weaknesses that may not be apparent to the audit team. Their in-depth knowledge of the processes allows them to pinpoint areas of risk and recommend appropriate audit procedures.
 - **Improving Testing Effectiveness:** SMEs can assist in the design and execution of audit tests, ensuring that the tests are relevant, effective, and efficient in achieving audit objectives.
- **Facilitating Communication:**
 - **Bridging the Gap:** SMEs can act as a bridge between the audit team and the business units, facilitating clear communication and understanding of audit procedures and findings.

- **Addressing Concerns:** SMEs can help address any concerns or questions raised by the business units during the audit process, ensuring a smooth and collaborative experience.
- **Validating Audit Findings:**
 - **Second Opinion:** SMEs can provide a second opinion on the audit findings, ensuring their accuracy and relevance. Their expertise can help validate the audit team's conclusions and identify any potential areas for further investigation.
- **Improving Audit Efficiency:**
 - **Streamlining Processes:** SMEs can help streamline the audit process by providing efficient and effective ways to gather evidence and perform audit procedures. This can save time and resources, allowing the audit team to focus on higher-risk areas.

By actively involving SMEs during the execution phase of an internal audit, organizations can significantly enhance the quality and effectiveness of the audit process, leading to more accurate and insightful findings, improved risk management, and greater assurance to stakeholders.

5.3.3 Reporting Phase:

SMEs participate in reviewing audit findings and contribute to the development of actionable recommendations. Here are some keyways they contribute:

- **Validating and Enhancing Audit Findings:**
 - **Technical Accuracy:** SMEs can review and validate the technical accuracy of the audit findings, ensuring that they are factually correct and reflect the actual situation.
 - **Contextualization:** SMEs can provide valuable context for the audit findings, explaining their implications for the business and the

potential impact on operations.

■ **Developing Meaningful Recommendations:**

- **Practical and Actionable:** SMEs can help develop practical and actionable recommendations for improvement, drawing on their in-depth knowledge of the business processes and industry best practices.
- **Prioritizing Recommendations:** SMEs can help prioritize recommendations based on their potential impact and feasibility, ensuring that management focuses on the most critical issues.

■ **Improving Communication and Understanding:**

- **Clear and Concise Reporting:** SMEs can help ensure that the audit report is clear, concise, and easy to understand for management.
- **Effective Communication:** SMEs can participate in the presentation of audit findings to management, facilitating a more effective and productive discussion.

■ **Ensuring Stakeholder Buy-in:**

- **Building Trust and Confidence:** By involving SMEs in the reporting phase, organizations can build trust and confidence in the audit findings among stakeholders.
- **Improved Communication:** SMEs can help bridge the communication gap between the audit team and management, ensuring that the audit findings are understood and accepted by all stakeholders.

■ **Driving Continuous Improvement:**

- **Implementing Recommendations:** SMEs can play a crucial role in supporting the implementation of audit recommendations, providing guidance and support to the business units.

- **Monitoring Progress:** SMEs can help monitor the progress of corrective actions and ensure that the recommendations are implemented effectively and efficiently.

By actively involving SMEs in the reporting phase of an internal audit, organizations can ensure that the audit findings are accurate, relevant, and actionable. This can lead to significant improvements in the organization's risk management and control environment, ultimately enhancing the overall value and impact of the internal audit function

5.4 Best Practices for Collaborating with SMEs:

5.4.1 Define Objectives Clearly:

- **Specificity:** Clearly outline the scope of work and desired outcomes for the SME engagement. Avoid vague or ambiguous objectives.
- **Alignment:** Ensure that the SME's involvement aligns directly with the overall audit objectives. This helps maintain focus and avoid unnecessary diversions.
- **Measurable Outcomes:** Define measurable outcomes for the SME's contribution. This helps track progress and evaluate the effectiveness of the engagement.

5.4.2 Integrate into Audit Teams:

- **Active Participation:** Seamlessly integrate SMEs into the audit team's activities.
- **Planning:** Involve SMEs in planning sessions to leverage their expertise in risk identification and scoping.
- **Fieldwork:** Allow SMEs to participate in fieldwork activities, such as interviews, observations, and document reviews.
- **Reporting:** Include SMEs in discussions related to the drafting of audit

reports and the formulation of recommendations.

- **Communication:** Foster open and frequent communication between auditors and SMEs. Encourage the sharing of information and perspectives throughout the audit process.

5.4.3 Continuous Training:

- **Audit Methodologies:** Provide SMEs with training on relevant audit methodologies, frameworks (e.g., COSO, ISO 9001), and professional standards.
- **Organizational Objectives:** Educate SMEs on the organization's strategic objectives, risk appetite, and key performance indicators. This helps them understand the broader context of the audit and contribute more effectively.
- **Industry Best Practices:** Keep SMEs updated on the latest industry best practices, regulations, and emerging risks. This ensures that their knowledge remains current and relevant.

5.4.4 Confidentiality and Independence:

- **Clear Expectations:** Clearly communicate confidentiality expectations to all SMEs involved in the audit process. Emphasize the importance of maintaining the integrity and objectivity of the audit.
- **Independence:** Ensure that SMEs maintain their independence and objectivity throughout the audit process. Avoid situations where SMEs may have conflicts of interest.
- **Regular Reviews:** Conduct regular reviews to ensure that confidentiality and independence are maintained throughout the engagement.

5.4.5 Feedback Mechanisms:

- **Regular Feedback:** Gather feedback from both auditors and SMEs after

each engagement. This provides valuable insights into the effectiveness of the collaboration and areas for improvement.

- **Actionable Insights:** Analyse feedback and implement appropriate changes to improve future SME engagements.
- **Continuous Improvement:** Use feedback to continuously improve the collaboration process and maximize the value that SMEs bring to the internal audit function.

By following these best practices, internal audit functions can effectively leverage the expertise of SMEs, enhance the quality and effectiveness of their audits, and ultimately improve the organization's risk management and control environment.

5.5 Strategies for Identifying the relevant SMEs:

5.5.1 Leverage Internal Resources:

- **Internal Referrals:** Utilize recommendations from colleagues or department heads who may have insights into potential SMEs within the organization. This can help ensure that the selected experts are already familiar with the company's operations and culture, enhancing their effectiveness.
- **Departmental Expertise:** Explore existing talent in various departments. Employees who specialize in specific processes or controls can provide valuable insights that are crucial for the audit.

5.5.2 Utilize Professional Networks:

- **LinkedIn and Professional Associations:** Use platforms like LinkedIn to search for professionals with expertise in relevant areas. Reviewing their profiles, publications, and past presentations can help validate their qualifications and suitability for the project.
- **Industry Events:** Attend conferences, webinars, and workshops to connect with potential SMEs. These events provide opportunities to assess their

communication skills and depth of knowledge in real-time.

5.5.3 Conduct Thorough Research:

- **Online Searches:** Perform targeted searches to find articles, white papers, or case studies authored by potential SMEs. This can provide insights into their expertise and contributions to their field.
- **Industry Events:** Attend conferences, webinars, and workshops to connect with potential SMEs. These events provide opportunities to assess their communication skills and depth of knowledge in real-time.

5.5.4 Assessment of Skills:

- **Evaluate Communication Skills:** Ensure that the SME not only possesses deep knowledge but also could convey that knowledge effectively to auditors and stakeholders.
- **Training Intake Forms:** Implement training intake forms that include questions about potential SMEs. This can facilitate quicker identification of suitable candidates during project planning stages.

5.5.5 Engage External Consultants When Necessary:

For specialized areas lacking internal expertise, consider bringing in external consultants with a proven track record in specific fields relevant to the audit scope. However, prioritize internal experts for high-impact projects where institutional knowledge is critical.

5.5.6 Feedback Mechanisms:

After engaging an SME, establish feedback mechanisms to evaluate their performance and contributions. This helps refine future selections and improve criteria for choosing SMEs.

5.6 Challenges in Utilizing SMEs:

While SMEs bring considerable value, organizations may encounter certain challenges:

- **Cost Implications:** SMEs often command higher compensation rates due to their expertise, potentially increasing audit budgets.
- **Availability Issues:** High demand for SMEs' expertise can lead to scheduling conflicts.
- **Integration Barriers:** Ensuring that SMEs' specialized knowledge aligns with the holistic perspective of internal audits requires careful coordination.

Conclusion:

Subject Matter Experts are invaluable allies in internal audit, offering the specialized knowledge necessary to navigate complex and dynamic business environments. By leveraging SMEs effectively, organizations can enhance the quality of their audits, ensure compliance, and achieve strategic objectives with greater precision and efficiency. Establishing robust practices for engaging SMEs today will position organizations for resilience and success in the years to come. The role of SMEs in internal audit will continue to grow as organizations face complex, interconnected risks. Advances in data analytics, regulatory scrutiny, and technological innovations will further amplify the need for expert guidance. Forward-looking audit functions should adopt a hybrid model, blending generalist auditors with SMEs to create agile, high-impact teams.

5.7 Key Areas Requiring Subject Matter Experts (SMEs):

In an era defined by rapid technological evolution, complex problem-solving, and a globalized economy, the demand for Subject Matter Experts (SMEs) has surged. These specialists play critical roles in driving innovation, improving operational efficiency, and ensuring informed decision-making across industries. Highlighting key areas that demand SMEs, offering insights into their contributions and the value they add.

5.7.1 Technology Audits:

As digital transformation accelerates, technology-related expertise has become crucial. Key areas include:

- **Artificial Intelligence and Machine Learning (AI/ML)**

- Developing predictive models and intelligent systems.
- Optimizing algorithms to tackle problems in healthcare, finance, and more.

- **Cybersecurity**

SMEs with expertise in cybersecurity, such as network security engineers, penetration testers, and data security analysts, can provide valuable insights into:

- Identifying and assessing cybersecurity risks, including vulnerabilities, threats, and potential attacks.
- Evaluating the effectiveness of security controls, such as firewalls, intrusion detection systems, and data encryption.
- Assessing compliance with data privacy regulations (e.g., GDPR, CCPA).

- **IT General Controls:**

SMEs with expertise in IT systems and controls can help assess the effectiveness of IT general controls, such as access control, change management, and systems development.

- **Data Analytics:**

Data scientists or analysts can help analyse large datasets to identify trends, anomalies, and potential risks.

■ **Cloud Computing and Infrastructure**

- Implementing scalable cloud solutions.
- Enhancing systems' reliability and security in hybrid environments.

Why SMEs Matter: The technology landscape changes rapidly, requiring experts who stay ahead of trends and threats to maintain system integrity and foster innovation.

5.7.2 Environmental, Health, and Safety (EHS) and Sustainability:

As concerns over climate change intensify, industries require experts to guide sustainable practices and innovations.

■ **Environmental Engineers:**

Environmental engineers can help assess compliance with environmental regulations, such as emissions standards and waste disposal regulations.

■ **Health and Safety Professionals:**

Health and safety professionals can help assess workplace safety hazards, evaluate the effectiveness of safety programs, and ensure compliance with occupational health and safety regulations.

■ **Energy and Waste Management**

- Developing solutions in wind, solar, and bioenergy.
- Improving energy storage and efficiency.
- Advocating for sustainable development policies.
- Restoring ecosystems and biodiversity.
- Innovating recycling techniques and reducing ecological footprints.

Why SMEs Matter: Sustainability experts address critical global challenges,

ensuring future generations inherit a liveable planet.

5.7.3 Finance Audits:

■ Accounting and Finance:

- SMEs with expertise in accounting, finance, and financial reporting can provide valuable insights into the accuracy and completeness of financial statements.
- The effectiveness of internal controls over financial reporting.
- The adequacy of financial risk management processes



■ Fraud Risk Management:

Forensic accountants or fraud examiners can help identify and assess fraud risks, such as financial statement fraud, corruption, and embezzlement.

■ Valuation and Appraisal:

SMEs with expertise in valuation and appraisal can provide insights into the accuracy and reliability of asset valuations.

Why SMEs Matter: SMEs play a crucial role in enhancing the quality and reliability of financial reporting and increase stakeholder confidence in the integrity of Organisation's financial statements.

5.7.4 Strategy and Business Modelling:

The complexity of modern financial systems necessitates experts to navigate economic trends and ensure compliance.

■ Financial Analytics

- Crafting predictive models for investment and risk management.
- Optimizing capital allocation strategies.

■ **Global Trade and Policy**

- Advising on international regulations and trade agreements.
- Managing supply chain complexities in global markets.

■ **Cryptocurrency and Blockchain**

- Enhancing secure, decentralized transaction mechanisms.
- Mitigating risks in digital asset ecosystems.

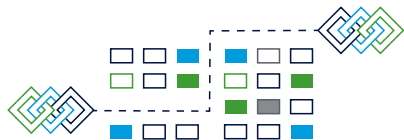
Why SMEs Matter: Experts in these domains help institutions manage risk, comply with regulations, and uncover economic opportunities.

5.7.5 Supply Chain Management:

In a globalized economy, managing supply chains efficiently is critical, and SMEs provide invaluable expertise in optimizing operations.

■ **Demand Forecasting**

- Utilizing advanced analytics to predict demand trends and prevent stockouts.
- Enabling agile responses to market fluctuations.



■ **Logistics Optimization**

- Streamlining transportation networks to minimize cost and delivery time.
- Implementing technologies such as RFID and IoT to enhance real-time tracking.

■ **Supplier Relationship Management**

- Developing strategic partnerships to ensure reliable supply.

- Evaluating and mitigating risks in supplier networks.

Why SMEs Matter: SMEs in supply chain management drive efficiency, reduce costs, and enhance resilience by leveraging their specialized knowledge in planning, logistics, and technology integration.

5.7.6 Customer Relationship Management (CRM):

Building strong and sustainable customer relationships is vital for long-term business success. SMEs in customer relationship management contribute by:

- **Data-Driven Insights**

- Analysing customer data to understand behaviours and preferences.
- Personalizing customer experiences to enhance satisfaction and loyalty.

- **CRM Technology Implementation**

- Deploying and optimizing CRM systems to streamline processes.
- Training teams to maximize the benefits of CRM tools.

- **Customer Retention Strategies**

- Crafting loyalty programs and targeted marketing campaigns.
- Addressing customer pain points promptly to improve engagement.

Why SMEs Matter: SMEs in CRM enhance customer satisfaction and retention through tailored strategies, fostering deeper connections and driving revenue growth.

5.7.7 Legal and Regulatory Compliance:

Navigating the regulatory landscapes across industries requires domain-specific legal expertise.

■ **Data Privacy and Protection**

- Ensuring compliance with laws like GDPR and DPDPA.
- Crafting privacy-first policies for organizations.

■ **Corporate Governance**

- Guiding ethical business practices.
- Creating robust frameworks to mitigate liability.

Why SMEs Matter: Legal experts safeguard organizations by managing risk and ensuring adherence to evolving laws.

5.7.8 Operational Audits:

■ **Production Processes & Quality Control:**

- **Understanding Complex Processes:** SMEs with expertise in manufacturing processes (e.g., chemical engineers, industrial engineers) can assess the efficiency of production workflows, identify bottlenecks, and evaluate the adequacy of process controls.
- **Quality Assurance:** They can review quality control procedures, assess the effectiveness of testing methods, and validate the accuracy of quality data. This ensures that products meet specifications and industry standards.
- **Advanced Technologies:** In industries with advanced technologies (e.g., robotics, automation), SMEs can assess the effectiveness of automated systems, identify potential risks associated with their implementation, and evaluate the integration of IoT devices.

■ **Maintenance & Reliability**

- **Equipment Maintenance:**

Engineers with expertise in equipment maintenance can assess the effectiveness of maintenance programs, identify potential equipment failures, and recommend preventive maintenance strategies.

➤ **Reliability Engineering:**

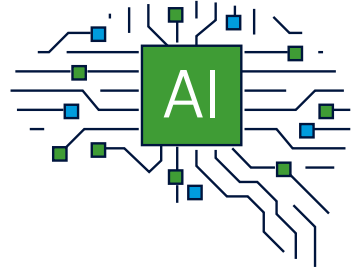
SMEs can help assess the reliability of equipment and systems, identify potential failure modes, and implement strategies to improve equipment uptime and reduce maintenance costs.

Why SMEs Matter: By effectively leveraging the expertise of SMEs in these technical areas, organizations can significantly enhance the value and impact of their operational audits, leading to improved performance, reduced risks, and increased competitiveness.

Conclusion:

Subject Matter Experts are the cornerstone of progress across industries, offering depth of knowledge and actionable insights to navigate complex challenges. As the global landscape evolves, investing in expertise and fostering knowledge-sharing will be pivotal to sustained growth and success of an Organisation.

Internal audit functions play a critical role in evaluating and improving an organization's risk management, control, and governance processes. In recent years, the advent of advanced technologies, including analytics, automation, and artificial intelligence (AAA), has transformed the way internal audits are conducted. These tools enhance the effectiveness, efficiency, and scope of audits, enabling auditors to deliver more value to their organizations. However, as these tools become more integrated into business processes, internal auditors must also address associated risks, including biases, data inaccuracies, and governance challenges.



As organizations continue to embrace digital transformation, the internal audit function is increasingly viewed as a strategic enabler. Leveraging AAA technologies not only improves the traditional audit processes but also ensures that organizations stay resilient and adaptable in a fast-evolving business environment. This section explores the multifaceted impact of analytics, automation, and AI in internal audits, offering insights into their applications, challenges, and opportunities.

6.1 Data Analytics Enabled Automation

6.1.1 Analytics in Internal Audit: Analytics involves the use of data and statistical techniques to uncover patterns, trends, and insights. In internal audit, analytics facilitates the examination of large datasets to identify anomalies, assess risks, and monitor controls.

6.1.2 Automation in Internal Audit: Automation refers to the use of technology to perform repetitive and rule-based tasks, freeing auditors to focus on higher-value activities. Key applications include:

- **Workflow Automation:** Automation streamlines audit planning, documentation, and reporting processes. For example, workflow automation tools can schedule tasks, send reminders, and consolidate audit

evidence automatically.

- **Robotic Process Automation (RPA) or Testing Automation:** RPA tools can extract and analyse data from various sources, reducing manual effort. These tools are particularly useful in handling structured tasks, such as reconciling accounts or validating invoices.

6.1.3 Why is Data Analytics used in Internal Audits?

- Data Analytics is an indispensable part of internal audits: It is a given fact that if internal audit has to provide assurance on effective functioning of controls, the use of data analytics is indispensable. Relying solely on substantive or sample testing, even with extensive coverage, may not provide sufficient assurance or confidence to the management on internal controls effectiveness.

Data analytics has become an integral part of internal audits and it is hard to imagine internal audits without data analysis.

- **Key benefits include:**
 - **Enhanced Risk Identification:** Analytics enables auditors to proactively identify potential risks by analysing historical and real-time data. For example, financial institutions utilize data analytics to detect unusual transactions that could indicate fraud or compliance breaches.
 - **Improved Audit Quality:** Data-driven insights lead to more accurate findings and recommendations. Through advanced visualization tools, auditors can present complex data in comprehensible formats for stakeholders.
 - **Continuous Monitoring:** Real-time analytics tools allow for ongoing oversight, reducing the lag between risk identification and response. For instance, dashboards powered by analytics provide continuous

updates on compliance metrics, enabling immediate corrective actions.

6.1.4 When Data Analytics can be used and to what extent?

- **At all stages of internal audit:** Data analytics is applied at all stages of the internal audit beginning from audit planning to risk assessment, test of controls, field work completion and reporting.
- **Factors governing usage of Data Analytics:** However, following are the factors that determine usage of data analytics in internal audits:
- **Availability of Quality Information determines the extent of usage of Data Analytics:**

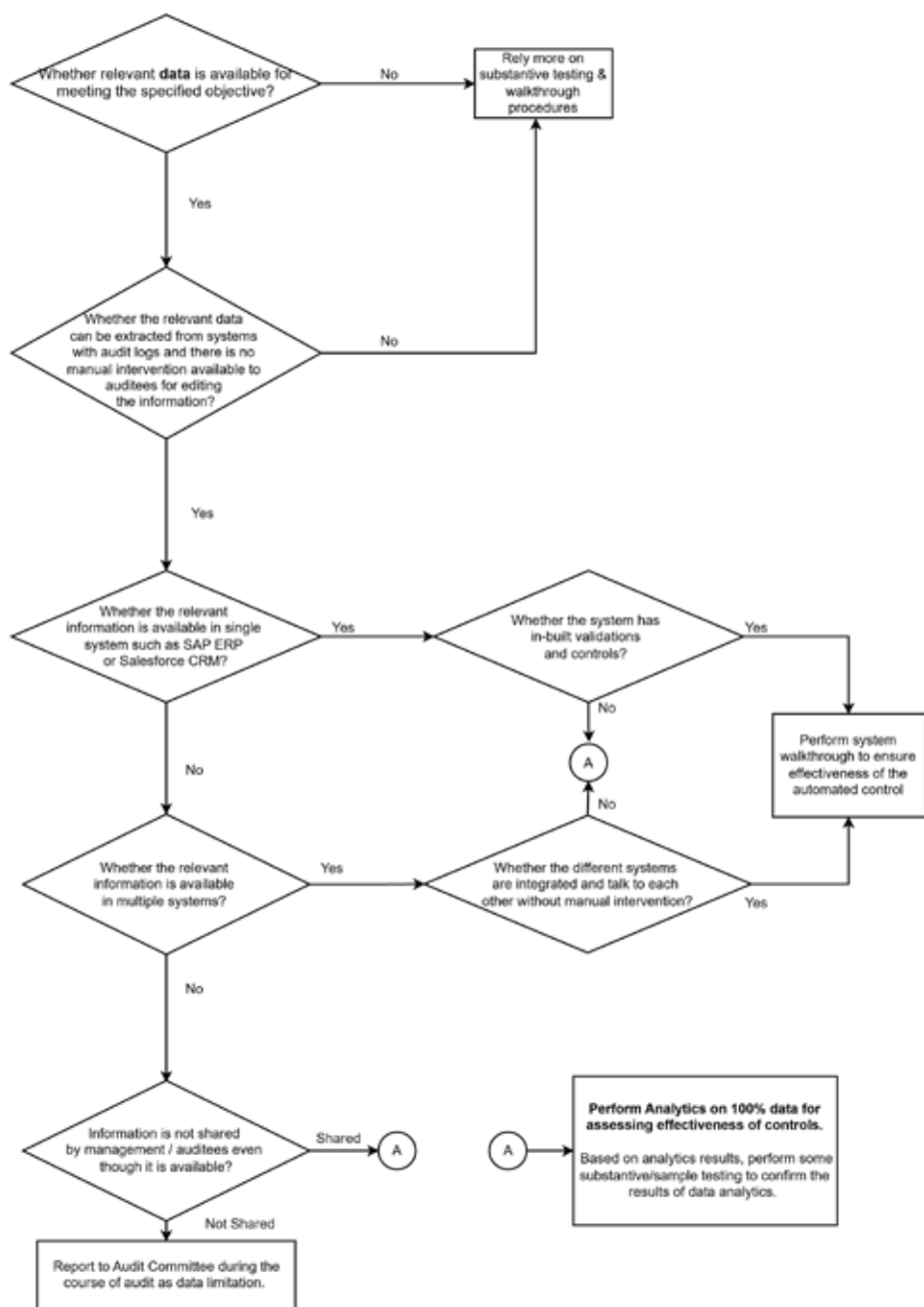
The extent to which data analytics is done depends on the availability of reliable data for the specified objectives of the internal audit.

➤ Information generated can be reliable if there is no manual intervention via human interface to edit the digitally generated information and edit logs are available in the system for the same.

➤ Information is captured in the system in a systematic matter – for example, if there is text captured the same is generally done in a predefined manner.

- **Systems used, automated controls inside the systems and integration of various systems:** Data analytics also plays a special role in today's digital environment specifically where data is generated and stored in various disparate systems that are not always integrated into a single data source. Just by reviewing the data together itself generates a lot of value for the company and management.

Following process chart summarizes the extent to which data analytics can be applied in internal audits and provides a framework for usage of data analytics in internal audits:



6.1.5 Challenges and Opportunities

While analytics and automation bring significant benefits, they also pose challenges, such as data reliability issues, complexity of databases, technology integration, and the need for upskilling auditors. Organizations must invest in robust data governance and continuous learning to harness the full potential of these tools.

- **Data Governance:** Establishing robust data governance frameworks ensures that analytics and automation tools rely on accurate, consistent, and secure data.
- **Training and Development:** Upskilling audit teams to understand and utilize advanced tools is crucial. Training programs focusing on data analytics and technology implementation enhance the overall capability of the audit function.

It is important to assess where analytics can be used based on the above decision tree. Due to emergence of analytical tools (refer Section 4.3) and the ability to quickly generate scripts using artificial intelligence, the opportunity to use data analytics in relevant circumstances has increased exponentially. Also due to increased usage of digital transactions across various sectors, and usage of number of specialised computing systems for different aspects of business environments, internal auditing will continue to rely on data analytics for times to come.

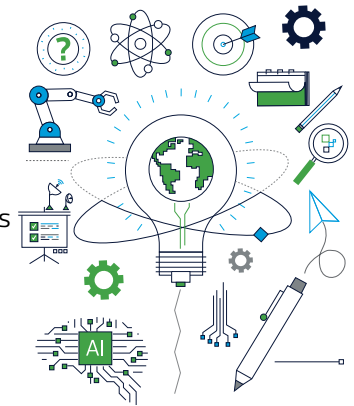
6.2 Artificial Intelligence in Internal Audit

6.2.1 Overview of AI in Internal Audit

Artificial intelligence (AI) encompasses technologies like machine learning, natural language processing, and cognitive computing. AI enables auditors to process complex datasets, detect emerging risks, and make informed decisions. However, risks such as data poisoning, bias in training data, and over-reliance on AI-generated insights must be managed carefully.

6.2.2 Generative AI, the game changer: The recent emergence of generative AI has been game changing not only for internal audit profession, but across various disciplines and industries.

Generative AI are algorithms which can be used to create new content, including audio, code, images, text, simulations, and videos. Generative AI systems fall under the broad category of machine learning and include large language models, but also many other applications. Generative AI is moving at fast pace and there are new fields and a huge number of organizations developing AI platforms, with both narrow and broad capabilities.



6.2.3 Why Generative AI should be used in Internal Audits?

A study by Arizona State University and Uniper, a large German multi-national energy company, states that “Uniper has implemented ChatGPT into parts of audit preparation, fieldwork, and audit reporting. On their initial tests, they estimate efficiency gains ranging from 50 to 80 percent for various processes”.

This is an example of the impact AI can have on Internal Audits in times to come.

6.2.4 How Generative AI can be used in Internal Audits?

Risk assessment	Audit plan development	Engagement planning	Execution	Reporting
Supporting auditor research and understanding of risk for a specific industry	Supporting auditor research and understanding on risk, business process and expected	Suggest test procedures based on in scope risk areas Suggest data sources, tables and	Analysis of data through natural language questioning Suggested interview questions	Initial draft report Editorial QA e.g. simplifying language, sentiment analysis

Risk assessment	Audit plan development	Engagement planning	Execution	Reporting
Supporting audit universe creation e.g. guidance on universe design, process universe, etc.	controls in advance of engagement planning Suggested audits against the risk assessed audit universe Suggested scheduling and resource allocation based on known constraints e.g. number and levels of staff	potential analytics tests Generate scripts for data extract and analytics execution First draft of scope/terms of reference	for different stakeholders Critical assessment of risk and control descriptions (e.g. if it covers who, what, where, when, etc.) Initial draft of workpaper Drawing themes from interview notes / audio Summation / interrogation of audit evidence documents Initial workpaper review and QA Initial draft of issues / observations.	Preparation of reports for Audit Committee summaries Generation of video/audio reporting Customised communications stakeholders' style Drafting emails to communicate the audit report

6.2.5 Examples or demonstrations of using Generative AI (ChatGPT) in Internal Audits

Case Study 1: Following is the input provided to ChatGPT for drafting list of controls to be tested based on walkthrough:

You are an internal auditor. The payroll process of the company is mostly manual and data sources are from different systems. Following is the detailed input:

- a. Attendance and leaves information comes from Biometric and an excel extract is passed on as input to the payroll team for processing.
- b. Joiners and exit data is maintained in Workday software and that information is extracted from by HR team and shared with payroll for considering new employees and holding payments for exits.
- c. additional allowances or salary payout over and above CTC are all manually provided to the Payroll team by HR.

Payroll is computed by a third party service provider named PaySquare. Can you provide a list of potential risks in a company's payroll process and suggest control tests that can be done for getting assurance and comfort on payroll process?

ChatGPT has returned the following output immediately:

1. Reconciliation of Attendance Records:

- **Test:** Regularly reconcile attendance records from the biometric system with the records submitted to PaySquare. This test ensures that the payroll calculations are based on accurate attendance data.
- **Objective:** To confirm the accuracy and completeness of attendance data used for payroll processing.

2. Verification of New Joiners and Exits:

- **Test:** Perform a monthly comparison of the joiners and exit reports from Workday with the payroll records to ensure all new employees are added and exiting employees are removed in a timely manner.
- **Objective:** To ensure that only eligible employees are receiving payments.

3. Review of Manual Adjustments and Allowances:

- **Test:** Implement a review process for manual adjustments and additional allowances entered by HR to confirm their authorization and accuracy.
- **Objective:** To detect and prevent unauthorized or erroneous payroll adjustments.

4. Compliance Check:

- **Test:** Conduct periodic audits to ensure payroll processing complies with relevant tax laws and employment regulations.
- **Objective:** To mitigate compliance risks and avoid potential penalties.

5. Fraud Detection Mechanisms:

- **Test:** Implement periodic, random audits of payroll records and establish a whistleblower policy to identify and investigate any potential payroll fraud.
- **Objective:** To detect and prevent fraudulent activities within the payroll process.

Case Study 2: Following input was given for doing vendor master analysis in python

I have a vendor code with following columns:

"No." - contains vendor code.

"Name" - vendor name

Address

Address 2

City

"Post Code" - vendor pin code

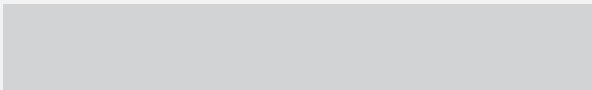
"PAN no." - vendor unique identification number as provided by government.

"GST Registration No." - vendor unique identification number as provided by government state wise.

Bank Account Number

"IFSC Code" - Branch code of the vendor where his bank account is maintained.

The vendor master is saved in the following path:



Need to identify following cases using python code:

- a. Duplicate Vendor codes within same city
- b. PAN not updated
- c. Vendors having same PAN but different names - use fuzzy technique with 80% confidence.
- d. GST No. not updated
- e. Same Bank A/c mapped to multiple vendors with different names - use fuzzy technique with 80% confidence.

ChatGPT returned the code which can correctly saving significant amount of time and also empowering auditors who do not have knowledge of python scripting or any other programming language. It also allowed time for creativity there-in tweaking the results. Sample output from ChatGPT is given below:



To identify the mentioned cases in the vendor code dataset using Python, you can utilize the pandas library for data manipulation and fuzzy matching techniques. Here's an example code that addresses each case:

```
python Copy

import pandas as pd
from fuzzywuzzy import fuzz

# Load the vendor code dataset
file_path = r'C:\Users\pariharm\OneDrive - Suresh Surana & Associates LLP\12. UrbanL\3. RS
sheet_name = 'vendorMaster'
df = pd.read_excel(file_path, sheet_name=sheet_name)

# Case a: Duplicate Vendor codes within the same city
duplicate_vendors = df[df.duplicated(subset=['No.', 'City'], keep=False)]
if not duplicate_vendors.empty:
    print("Duplicate Vendor codes within the same city:")
    print(duplicate_vendors[['No.', 'Name', 'City']])

# Case b: PAN not updated
pan_not_updated = df[df['PAN no.'].isnull()]
if not pan_not_updated.empty:
    print("Vendors with PAN not updated:")
    print(pan_not_updated[['No.', 'Name']])

# Case c: Vendors having the same PAN but different names using fuzzy technique
def fuzzy_match_names(row):
    similar_ratio = fuzz.token_sort_ratio(row['Name'], row['Name_match'])
    return similar_ratio >= 80

df['Name_match'] = df['Name']
duplicate_pans = df[df.duplicated(subset='PAN no.', keep=False)]
duplicate_pans['Name_match'] = duplicate_pans.groupby('PAN no.')['Name_match'].transform('
same_pans_diff_names = duplicate_pans[duplicate_pans.apply(fuzzy_match_names, axis=1)]
if not same_pans_diff_names.empty:
    print("Vendors having the same PAN but different names:")
    print(same_pans_diff_names[['No.', 'Name', 'PAN no.', 'Name_match']])
```

Message ChatGPT



6.2.6 Model evaluation using airtrain.ai

Since the generative AI models are trained on separate set of information, it is likely that a particular model may be good for a particular task say drafting observations in power point and a different model may be good for another task say research work.

Airtain.ai can be used to simultaneously test the results of a particular prompt to determine the best tool for a particular activity.

6.2.7 The risks of using Generative AI tools and suggested measures

Generative AI is impressive. The ability of technologies such as large language models to provide coherent and insightful responses, in a human like dialogue. This can quickly lead to high levels of trust being placed in their output. Functions who choose to ignore these technologies will fall behind, but their adoption of them must be managed and considered. Following are the risks foreseen and suggested measures:

Risk Foreseen	Suggested Risk Mitigation Measure
Accuracy: Gen AI can sometimes generate outputs that are factually incorrect, misleading or inappropriate.	Fact checks the outputs of Gen AI with subject matter experts.
Traceability: Gen AI tools are often “black boxes,” making it difficult to understand how they arrive at particular outputs.	Maintain a healthy level of professional scepticism.
Intellectual property infringement: Tools may have been trained on and plagiarize existing content, leading to potential legal issues.	Use Gen AI as an accelerator rather than a replacement of human involvement.
Data security loss: Sensitive or confidential information could inadvertently leave the organisation where public tools are used.	Set clear guidelines on when and how staff should use such tools. When information is being uploaded to the Generative AI tools, ensure confidential and private information is redacted carefully before uploading.

Risk Foreseen	Suggested Risk Mitigation Measure
Bias Propagation: Gen AI can perpetuate and even amplify existing biases in the data they were trained on.	Maintain a healthy level of professional scepticism.

6.2.8 Challenges and Opportunities




Generative AI is rapidly transforming industries, and internal audit is no exception. By leveraging its capabilities, organizations can enhance audit processes, identify risks more effectively, and generate insights from vast amounts of unstructured data. However, alongside these opportunities come significant challenges that require thoughtful navigation.

Generative AI can analyse documents, extract critical information, and even draft initial audit reports, freeing up auditors to focus on higher-value activities like strategic risk analysis.

Data security is one of the major pressing concerns, as sensitive organizational information processed by AI systems may be vulnerable to breaches. Organizations must balance these risks against the benefits to ensure AI adoption enhances the effectiveness and credibility of their internal audit functions.

6.3 Tools Deployed for Analytics and Automation in Internal Audit

Internal Auditors generally wide ranging tools for data analytics and automation in internal audit:

Rule Processing Analytics: These tools help in identifying patterns, exceptions, and trends within datasets by applying pre-defined or custom rules to large volumes of data.	Data Visualization Tools: These tools are used to create interactive dashboards and visualizations, enabling auditors to identify insights and trends quickly.
Programming Languages / Databases: Python is used for advanced analytics, scripting, and machine learning, while SQL is essential for querying and managing relational databases.	Traditional or Basic Tools such as Microsoft Excel: A widely used tool for basic data analysis, pivot tables, and managing smaller datasets. Also, there are add-ins available for using ChatGPT inside Microsoft excel.
Audit Reporting Tools: These tools facilitate tracking and monitoring of audit findings and action plans, ensuring accountability and closure.	Robotic Process Automation (RPA) Tools: These tools are leveraged to automate repetitive audit tasks, enhance efficiency, and reduce manual effort.
Generative AI Tools such as ChatGPT, Google Gemini, or Microsoft Copilot: These tools assist in drafting audit reports, summarizing key findings, automating documentation, and generating insights from data. Also, the ICAI has released GPTs customized for internal audit profession. To effectively use the tools in 6 different segments mentioned above, Generative AI tools can be used to enhance productivity and creativity in Internal Audits.	
<div><div> Gemini</div><div> Copilot</div><div></div><div><div>ICAI Internal Audit GPT</div><div>▼</div></div></div>	

6.4 Auditing in an Artificial Intelligence Environment

6.4.1 The Evolving Audit Landscape

As organizations adopt AI technologies, internal auditors must adapt their methodologies to address new challenges. Auditing in an AI environment requires an understanding of AI systems, data governance, and ethical considerations.

6.4.2 Key Considerations for Auditing AI Systems

- **Algorithm Integrity:** Auditors must assess the design, training, and testing of AI algorithms to ensure reliability and fairness.
- **Data Governance:** Strong data management practices are critical for ensuring the accuracy and security of AI inputs and outputs.
- **Bias and Ethics:** Auditors should evaluate AI systems for potential biases and ethical implications, ensuring compliance with relevant regulations.
- **Explainability:** AI models must be interpretable, enabling auditors to understand how decisions are made.
- **Data Security Risks:** Address potential risks such as inadvertent data sharing with external AI tools and ensure strict compliance with data privacy laws.



6.4.3 Challenges and Opportunities

Auditing AI systems presents challenges, such as the complexity of algorithms, rapid technological changes, and limited expertise. However, it also offers opportunities to enhance audit precision, scope, and relevance. Continuous learning and collaboration are essential for auditors to succeed in this evolving

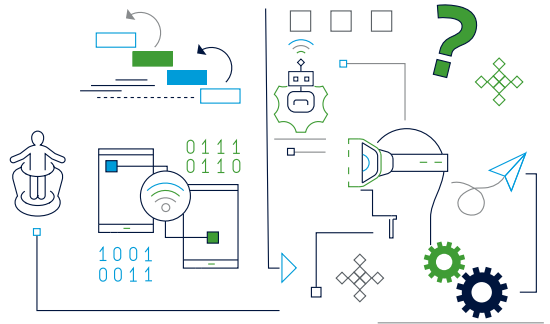
landscape.

Conclusion

The integration of analytics, automation, and artificial intelligence into internal audit functions represents a paradigm shift. These technologies enable auditors to uncover deeper insights, respond to risks more effectively, and deliver greater value to their organizations. To address inherent risks like biases and ethical challenges, internal auditors must maintain professional scepticism and leverage robust frameworks.

As the adoption of AAA technologies accelerates, the internal audit profession must evolve to match the pace of innovation. This includes developing forward-looking audit plans, fostering a culture of continuous learning, and maintaining agility in the face of technological advancements. The future of internal audit lies in its ability to integrate these cutting-edge tools while safeguarding organizational integrity and resilience.

The Digital and Mobility revolution has improved, impacted as well as disrupted business models, processes and efficiencies. The emergence of e-commerce, mobile applications, sophisticated ERPs, block chain solutions, cloud computing, robotic business process automation (RPA), internet of things (IoT), machine learning and artificial intelligence (AI)



have added and will add new dimensions to businesses. The internal audit function needs to re-orient itself to meet the requirements in this Digital Era as well as improve its own approach and methodology.

Some of the key questions around Information Technology (IT) risk management and Internal Audit that organisations face in today’s disruptive environment are as follows:

- Are the controls and Segregation of Duties (SoDs) mapped correctly in your IT/ ERP systems? What are the over-rides and the mechanisms for audit trails of such over-rides?
- Does your audit plan identify key IT risks that have direct significant impact on the organisation?
- Is IT audit part of your internal audit plan?
- Have you identified opportunities to reduce manual controls by increasing automated controls?
- Have you identified areas in your internal audit plan where data analytics can be used for the audit of complete or larger set of data set rather than sample based approach?
- Have you assessed the business, financial, legal and reputational risks associated

with data leakage or cyber frauds? Have your effective control and audit mechanisms in place to counter the same?

- Have you ascertained applicable data privacy regulations and put in place the mechanism required to conform to the same? Are the same covered in the internal audit and/or IT systems audit?
- Have you identified the laws requiring digital filings and reporting? Are their effective controls for the digital authorization of the filings (DSCs), review of compliances, receipt and adherence to any on-line notices/proceedings, etc.?
- Have you identified areas in your audit plan where technology can be used to evaluate the effectiveness of controls against the key risks?
- Does your Internal Audit team have sufficient IT competencies to evaluate the effectiveness of controls?
- Do you have a program/framework established to ensure the above aspects are verified on a continual basis?

7.1. Information Technology in Internal Audit – A Key Differentiator

- Internal audits are designed to evaluate the effectiveness of organisation's internal controls by first gathering information about how a unit operates, identifying points at which errors or inefficiencies are possible and identifying system controls designed to prevent or detect such occurrences. Then, the application and performance of those controls are tested to assess how well they work. Managers ought to routinely evaluate controls in their department's operations by following the same process.
- IT provides most of the information needed for auditing. In order to be effective, auditors must use IT as an auditing tool, audit automated systems and data, to understand the business purposes for the systems, and understand the environment in which the systems operate.

- The other important uses of IT by auditors are in audit administration. By seeking new use for computers and communications, auditors improve their ability to review systems and information and manage their activities more effectively. Automated tools allow auditors to increase individual productivity and that of the audit function. By recognising the importance of emerging environment and requirement to perform audit task effectively, auditors must recognise the key reasons to use audit tools and software.
- Some of the examples below demonstrate the need for an effective Internal Audit function leveraging technology platform.

7.2. Key IT considerations for Internal Audit

7.2.1. Information Security

Information Security	Key IT Internal Audit Considerations
Information security program assessment – Evaluates the organisation's information security program, including strategy, awareness and training, vulnerability assessments, predictive threat models, monitoring, detection and response, technologies and reporting.	<ul style="list-style-type: none">● How comprehensive is the existing information security program?● Is information security embedded within the organisation, or is it an "IT only" responsibility?● How well does the organisation self-assess threats and mitigate the threats?● How well the organisation finds the vulnerabilities and the solution for that?
Threat and vulnerability management program assessment –Evaluates the organisation's Threat and Vulnerability Management (TVM) program including threat intelligence, vulnerability identification, remediation, detection, response, and countermeasure planning.	<ul style="list-style-type: none">● How comprehensive is the existing TVM program?● Is the TVM program aligned with business strategy and the risk appetite of the organisation?● Are the components of TVM integrated with one another, as well as with other security and IT functions?● Do processes exist to make sure identified issues are appropriately addressed and remediation is effective?● What counter measures have been planned for the threats with the TVM?

7.2.2. Business Continuity Management

Business Continuity Management	Key IT Internal Audit Considerations
Business continuity program integration and governance audit – Evaluates the organisation's overall business continuity plan, including program governance, policies, risk assessments, business impact analysis, vendor / third-party assessment, strategy / plan, testing, maintenance, change management and training / awareness	<ul style="list-style-type: none">● Does a holistic business continuity plan exist for the organisation?● How does the plan compare to leading practice?● Is the plan tested?● What impact the plan and how the plan will affect the business?
Disaster recovery audit – Assesses IT's ability to effectively recover systems and resume regular system performance in the event of a disruption or disaster.	<ul style="list-style-type: none">● Are disaster recovery plans aligned with broader business continuity plans?● Do testing efforts provide confidence systems that can be effectively recovered?● Are all critical systems included? Are critical systems defined?
Crisis management audit – Reviews the organisation's crisis management plans, including overall strategy / plan, asset protection, employee safety, communication methods, public relations, testing, maintenance, change management and training / awareness.	<ul style="list-style-type: none">● Are crisis management plans aligned with broader business continuity plans?● Are plans comprehensive and do they involve the right corporate functions?● Are plans well communicated?

7.2.3. Mobile Security

Mobile Security	Key IT Internal Audit Considerations
Mobile device configuration review – Identifies risks in mobile device settings and vulnerabilities in the current implementation. This audit would include an evaluation of trusted clients, supporting network architecture, policy implementation, management of lost or stolen devices, and vulnerability identification through network	<ul style="list-style-type: none">● How has the organisation implemented "bring your own device" (BYOD)?● Are the right policies / mobile strategies in place?● Are mobile devices managed in a consistent manner?● Are configuration settings secure and enforced through policy?

Mobile Security	Key IT Internal Audit Considerations
accessibility and policy configuration.	<ul style="list-style-type: none">● How do we manage lost and stolen devices?● What vulnerabilities exist, and how do we manage them?
Mobile application black box assessment – Performs audit using different front-end testing strategies: scan for vulnerabilities using various tools, and manually verify scan results. Attempts to exploit the vulnerabilities identified in mobile web apps.	<ul style="list-style-type: none">● What vulnerabilities can be successfully exploited?● How do we respond when exploited, and do we know an intrusion has occurred?
Mobile application grey box assessment – Combines traditional source code reviews (white box testing) with front-end (black box) testing techniques to identify critical areas of functionality and for symptoms of common poor coding practices. Each of these “hot spots” in the code should be linked to the live instance of the application where manual exploit techniques can verify the existence of a security vulnerability relations, testing, maintenance, change management and training/awareness.	<ul style="list-style-type: none">● How sound is the code associated with the mobile applications used within the organisation?● What vulnerabilities can be exploited within the code?● Whether OWASP top 10 vulnerabilities are present in the code?
Device Security configuration	<ul style="list-style-type: none">● Have your IT servers, infrastructure securely hardened?● Are the security patched updated appropriately?● Do you follow leading industry practices to secure systems?

7.2.4. Cloud Security

Cloud Security	Key IT Internal Audit Considerations
Cloud strategy and governance audit – Evaluates the organisation's strategy for utilizing cloud technologies. Determines whether the appropriate policies and controls have been	<ul style="list-style-type: none">● Are there supporting policies to follow when using a cloud provider?● Are policies integrated with legal, procurement and IT policies?

Cloud Security	Key IT Internal Audit Considerations
developed to support the deployment of the strategy. Evaluates alignment of the strategy to overall company objectives and the level of preparedness to adopt within the organisation.	<ul style="list-style-type: none">● How to make the organisation to adopt the changes?
Cloud security and privacy review – Assesses the information security practices and procedures of the cloud provider. This may be a review of their SOC 1, 2 and/or 3 report(s), a review of their security SLAs and/or an on-site vendor audit. Determines whether IT management worked to negotiate security requirements into their contract with the provider. Reviews procedures for periodic security assessments of the cloud provider(s), and determine what internal security measures have been taken to protect company information and data.	<ul style="list-style-type: none">● Does your organisation have secure authentication protocols for users working in the cloud?● Have the right safeguards been contractually established with the provider?
Cloud provider service review – Assesses the ability of the cloud provider to meet or exceed the agreed-upon SLAs in the contract. Areas of consideration should include technology, legal, governance, compliance, security and privacy. In addition, internal audit should assess what contingency plans exist in case of failure, liability agreements, extended support, and the inclusion of other terms and conditions as part of the service contracts, as well as availability, incident, and capacity management and scalability.	<ul style="list-style-type: none">● What SLAs are in place for uptime, issue management and overall service?● Has the cloud provider been meeting or exceeding the SLAs?● What issues have there been?● Does the organisation have an inventory of uses of external cloud service providers, sponsored both within IT and directly by the business units?

7.2.5. Social Media Risk Management

Social Media Risk Management	Key IT Internal Audit Considerations
Social media risk assessment – Collaborates with the IT organisation to assess the social media activities that would create the highest level of risk to the organisation. Evaluates the threats to the organisation's information security through the use of social media. This audit may be combined with a social media governance audit to then confirm policies have been designed to address the highest risks to the organisation.	<ul style="list-style-type: none">● Has the organisation identified what risks exist related to social media?● How well are the identified risks managed or mitigated?● Does the organisation periodically conduct a social media audit?
Social media governance audit – Evaluates the design of policies and procedures in place to manage social media within the organisation. Reviews policies and procedures against leading practices.	<ul style="list-style-type: none">● Does a governance process exist for social media within the organisation?● How well are policies related to social media known amongst employees?
Social media activities audit – Audits the social media activities of the organisation and its employees against the policies and procedures in place. Identifies new risks and assist in developing policies and controls to address the risks.	<ul style="list-style-type: none">● Are social media activities aligned to policy?● What corrective actions need to be put in place given activity?● How does existing activity affect brand and reputation?

7.2.6. Segregation of Duties & Identity Access Management (SoD & IAM)

Cloud Security	Key IT Internal Audit Considerations
Systematic segregation of duties review audit – Evaluates the process and controls IT has in place to effectively manage segregation of duties. Performs an assessment to determine where segregation of duties conflicts exist and compare to known conflicts communicated by IT. Evaluates the controls in place to manage risk	<ul style="list-style-type: none">● How does IT work with the business to identify cross application segregation of duties issues?● Are business personnel adequately informed of the ERP roles well enough to perform user access reviews?● While compensating controls identified for SoD conflicts may

Cloud Security	Key IT Internal Audit Considerations
where conflicts exist	detect financial misstatement, would they truly detect fraud?
Role design audit – Evaluates the design of roles within ERPs and other applications to determine whether inherent SoD issues are embedded within the roles. Provides role design, role clean-up or role redesign advisory assistance and pre- and post-implementation audits to solve identified SoD issues.	<ul style="list-style-type: none">● Does the organisation design roles in a way that creates inherent SoD issues?● Do business users understand the access being assigned to roles they are assigned ownership of?
Segregation of duties remediation audit – Follows up on previously identified external and internal audit findings around SoD conflicts.	<ul style="list-style-type: none">● Does the organisation take appropriate action when SoD conflicts are identified?● Have we proactively addressed SoD issues to prevent year-end audit issues?
IAM/GRC technology assessment – Evaluates how IAM or GRC software is currently used, or could be used, to improve SoD controls and processes.	<ul style="list-style-type: none">● Is IAM or GRC software currently used effectively to manage SoD risk?● What software could be utilised to improve our level of SoD control, and what are our business requirements?

7.2.7. Data Loss Prevention (DLP) and Privacy

Data Loss Prevention and Privacy	Key IT Internal Audit Considerations
Data governance and classification audit – Evaluates the processes management has put in place to classify data, and develop plans to protect the data based on the classification	<ul style="list-style-type: none">● What sensitive data do we hold – what is our most important data?● Where does our sensitive data reside, both internally and with third parties?● Where is our data going?
DLP control review – Audits the controls in place to manage privacy and data in motion, in use and at rest. Considers the following scope areas: perimeter security, network monitoring, use of instant messaging, privileged user monitoring, data sanitation, data redaction, export/save	<ul style="list-style-type: none">● What controls do we have in place to protect data?● How well do these controls operate?● Where do our vulnerabilities exist, and what must be done to manage these gaps?

Data Loss Prevention and Privacy	Key IT Internal Audit Considerations
control, endpoint security, physical media control, disposal and destruction, and mobile device protection.	
Privacy regulation audit – Evaluates the privacy regulations that affect the organisation, and assess management’s response to these regulations through policy development, awareness and control procedures.	<ul style="list-style-type: none">● How well do we understand the privacy regulations that affect our global business? For example, HIPAA is potentially a risk to all organisations, not just health care providers or payers or GDPR is applicable to organizations even if they do not have operations in the EU?.● Do we update and communicate policies in a timely manner?● Do users follow control procedures to address regulations?

7.2.8. Machine Learning

Machine Learning in Internal Audit	Key IT Internal Audit Considerations
Machine learning technology helps in finding the unstructured data, which include the emails and the social media posts and review them.	<ul style="list-style-type: none">● What controls do we have in place to protect unstructured data e.g. emails?● Is there any important data leaking out through social media?● Where is our data going?
Machine learning may be applied to help with the classification of transactions. Inductive reasoning could be applied to the source data of historical transactions to help “predict” the classification of additional transactions as they are recorded	<ul style="list-style-type: none">● What is the historical transaction pattern?● How the transactions are been classified?● What are the controls to protect the historical transaction data?
Machine learning has the ability of the computer to recognize and apply patterns, derive its own algorithms based on those patterns, and refine those algorithms based on feedback	<ul style="list-style-type: none">● What is the pattern of data been processed?● What type of algorithms in place for analysis so it meet the requirements?● Does any feedback mechanism been carried?

7.2.9. Block Chain

Block Chain in Internal Audit	Key IT Internal Audit Considerations
In a block chain system, the ledger is replicated in a large number of identical databases, each hosted and maintained by an interested party. When changes are entered in one copy, all the other copies are simultaneously updated. So as transactions occur, records of the value and assets exchanged are permanently entered in all ledgers.	<ul style="list-style-type: none"> ● What Existing policies and procedures will need to be updated to accommodate blockchain protocols and integrate blockchain transactions into legacy systems?
Blockchain technology help to test the whole population of transactions within the period under observation. This extensive coverage will drastically improve the level of assurance gained in affected audit engagements.	<ul style="list-style-type: none"> ● What type of data is processed? ● Is the data structured or unstructured? ● What controls do we have in place to protect data?
Blockchain Uses the encryption technology which help to secure the data.	<ul style="list-style-type: none"> ● What Credential and key management is crucial to protecting the digital assets stored on the blockchain? ● Who will have access to the data and encryption keys?

7.2.10. Robotics Process Automation

Robotics Process Automation	Key IT Internal Audit Considerations
RPA is configurable software, that work on the existing IT infrastructure, pulling data, performing algorithms, and creating reports. It uses business rules, can be configured to performed a variety of processes enabling multi-use robots, and variability as your business needs change.	<ul style="list-style-type: none"> ● Does the present infrastructure support RPA? ● What are the Data Governance and Controls Standards in the context of RPA? ● What Privacy and Data Protection the organisation follow in the context of RPA? ● Have optimised processes before we automated?
RPA offers broader spectrum of internal and external application integration in risk. It help to create document	<ul style="list-style-type: none"> ● What level of control implemented to organisation on the integration of application?

Robotics Process Automation	Key IT Internal Audit Considerations
repositories and connections to existing governance, risk and control (GRC) platforms that are linked to processes, risks and controls to demonstrate framework adherence and evidence traceability.	● Do business users understand the access being assigned to roles they are assigned ownership of?

7.3. Digital Personal Data Protection Act, 2023:

Data privacy, also referred to as information privacy or data protection, involves the proper handling, processing, storage, and dissemination of personal data. It encompasses the relationship between data collection practices, technology, public expectations, contextual information norms, and the legal and political frameworks that govern these activities.

The significance of data privacy has escalated in recent years due to the exponential increase in the volume and variety of personal information being collected and processed in the digital age.

The importance of data privacy can be understood through several key aspects:

- **Protecting personal information:** Ensures confidentiality and security of sensitive personal data, such as financial records, health information, and personal communications.
- **Maintaining trust:** Builds and sustains trust between individuals and organizations by guaranteeing responsible data handling.
- **Preventing abuse:** Protects against the misuse of personal information, such as identity theft, fraud, and unauthorized surveillance.
- **Compliance:** Ensures adherence to legal and regulatory mandates that require the protection of personal data.

India's Digital Personal Data Protection Act (DPDPA) was introduced in August, 2023 to regulate the processing of digital personal data while respecting

individuals' right to privacy and processing such data for lawful purposes. It aims to ensure transparency and accountability in data handling practices, aligning with global data protection standards. Further, draft rules for DPDPA were published on January 03, 2025.

7.3.1. Scope and Applicability:

- **Geographic Scope:** Applies to entities in India and those outside India processing personal data of individuals within India where the personal data is collected:
 - In digital form; or
 - In non-digital form and digitized subsequently.
 - Also applies to processing of digital personal data outside the territory of India, if such processing is in connection with any activity related to offering of goods or services to Data Principals within the territory of India.
- **Entities Covered:**
 - **Data Fiduciaries:** Individuals or organizations that determine the purpose and means of processing personal data.
 - **Data Processors:** Entities processing data on behalf of data fiduciaries.
- **Data Coverage:**

Governs personal data (identifiable information) and sensitive personal data (e.g., health, financial, biometric data).
- **Exemptions:**
 - Personal data processed by an individual for any personal or domestic purpose; and

- Personal data that is made or caused to be made publicly available by:
 - The Data Principal to whom such personal data relates; or
 - Any other person who is under an obligation under any law for the time being in force in India to make such personal data publicly available.

- **Cross-Border Transfers:**

Establishes requirements for transferring personal data outside India, ensuring compliance with protection standards.

7.3.2. Key Features:

- **Data Principal Rights:** Access, correction, erasure, portability, and consent withdrawal.
- **Data Fiduciary Responsibilities:** Organizations must implement security measures, ensure transparency, and notify individuals about data processing.
- **Consent:** Informed and revocable consent required before data collection.
- **Regulatory Authority:** Establishes a Data Protection Board for compliance oversight and grievance handling.
- **International Data Transfers:** Sets conditions for transferring personal data outside India.

7.3.3. Grounds for processing personal data: –

A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and for a lawful purpose,

- for which the Data Principal has given his/her consent; or

- for certain legitimate uses.

For the purposes of this section, the expression “lawful purpose” means any purpose which is not expressly forbidden by law.

7.3.4. Consent Management:

Obtaining and managing consent is a critical aspect of compliance:

- Consent must be obtained for all the cases except legitimate uses – (Refer Section 4(b) of the Act).
- Organizations must maintain records of consent to demonstrate compliance.
- Organizations shall develop a consent management system to comply with all the requirements stated in the obligations of Data Fiduciary.

Data Fiduciaries can process the personal data of Data Principal only when:

- Data Principal has given the consent or
- Data processing is covered under “Certain legitimate uses”.

7.3.5. Consent Mechanism:

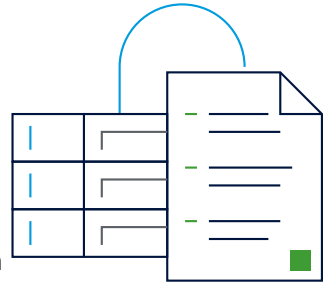
For obtaining the consent from Data Principal, Data Fiduciary shall give a notice containing the following information: –

- The personal data and the purpose for which the same is proposed to be processed.
- The manner in which consent can be withdrawn.
- Details of grievance redressal mechanism.
- The manner in which Data Principal may make a complaint to the data protection board.

If the consent is taken before the commencement of the DPDPA, then fresh notice needs to be issued in the above manner.

7.3.6. Requisites of consent:

- Consent shall be specific, informed, unconditional, independent and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of personal data for the specified purpose and not any other purposes. Any part of the consent which constitutes an infringement of the provisions of this Act, or the rules made thereunder or any other law for the time being in force shall be invalid to the extent of such infringement.
- The notice for consent must include the itemised description of personal data, specified purpose of, and an itemised description of the goods or services to be provided or uses to be enabled by, such processing.
- Shall be presented in a clear and plain language, giving the option to access such request in English or any language specified in the Eighth Schedule to the Constitution.
- Provide a particular communication link for accessing the website or app, or both, of such Data Fiduciary provided, using which such Data Principal may:
 - withdraw her consent, with the ease of doing so being comparable to that with which such consent was given;
 - exercise her rights under the Act; and
 - make complaint to the Board
- Provide the contact details of a Data Protection Officer, where applicable, or of any other person authorized by the Data Fiduciary to respond to any communication from the Data Principal.



- Verify the consent of the parent / legal guardian before processing any personal data of a child / person with disability through identify issued by Central / State Government or entrusted by law?

7.3.7. Change / withdrawal of consent:

- Right to manage, review or withdraw the consent with the same ease of providing the consent.
- If the Data Principal withdraws consent, Data Fiduciary shall cease processing of the data within a reasonable time.
- The consequences of the withdrawal shall be borne by the Data Principal, and such withdrawal shall not affect the legality of processing of the personal data based on consent before its withdrawal.

7.3.8. Certain Legitimate uses:

Data Fiduciary can process the personal data of Data Principal without consent if the processing falls under any of the following uses: –

- Voluntarily provided by the Data Principal for any specified purpose.
- Government services like subsidy, benefits, certificate, license etc.,
- If required by the government under any law.
- For fulfilling any obligation under any law.
- For the compliance of Judgement or Decree or order under any law.
- In case of medical emergencies like covid or any other pandemic.
- Health services during epidemic or any other threats to public health.
- For safety during disaster or any breakdown.
- For purposes of employment or those related to safeguarding the employer from loss or liability, such as prevention of corporate espionage, intellectual

property, classified information etc.

Regardless of the lawful basis for collecting data (whether it is for legitimate use, consent, legal obligations, etc.), organizations are required to implement adequate security measures to protect that data from unauthorized access, breaches, and other risks.

7.3.9. Data Security Measures:

Implementing robust security measures is essential to protect personal data from breaches and unauthorized access. Examples of such measures include:

- Use encryption and pseudonymization to protect data.
- Conduct regular security audits and vulnerability assessments.
- Implement access controls to ensure that only authorized personnel have access to data.
- Obtain ISO 27001 certification for information security management systems and ISO 27701 for privacy information management.

7.3.10. Penalties for non – compliance:

Non-compliance with the DPDPA can result in significant penalties, which are intended to deter violations and promote adherence to data protection standards. Penalties include:

S. No	Breach of provisions of this Act or rules made thereunder	Penalty
1	Breach in observing the obligation of Data Fiduciary to take reasonable security safeguards to prevent personal data breach.	May extend to two hundred and fifty crore rupees.
2	Breach in observing the obligation to give the Board or affected Data Principal notice of a personal data breach.	May extend to two hundred crore rupees
3	Breach in observance of additional obligations in relation to processing of personal data of children	May extend to two hundred crore rupees.

S. No	Breach of provisions of this Act or rules made thereunder	Penalty
4	Breach in observance of additional obligations of Significant Data Fiduciary	May extend to one hundred and fifty crore rupees.
5	Breach of any other provision of this Act or the rules made thereunder	May extend to fifty crore rupees.

7.3.11. Sectors which may be heavily impacted due to DPDP Act:

- Social Media platforms
- E-commerce websites
- Healthcare providers
- Financial services
- Telecommunication companies
- Travel & Hospitality services
- Education Technology companies
- Online entertainment & streaming services
- Online advertising

7.3.12. Ensuring data privacy through cybersecurity:

Ensuring data privacy through cybersecurity involves a combination of policies, practices, and technologies designed to protect personal and sensitive information from unauthorized access, disclosure, alteration, and destruction. Following are some key measures to ensure data privacy through security measures:

- **Developing cybersecurity strategy:**
 - Conducting joint risk assessments to identify and evaluate risks related to both cybersecurity and data privacy.
 - Establishing clear security policies outlining the rules for network

access, data protection, incident management etc.,

- Adopting established cybersecurity and data privacy frameworks such as ISO 27001, ISO 27701, NIST etc.,

■ **Implementing robust access controls:**

- Enforcing multi factor authentication for users having access to sensitive systems and data.
- Limiting access based on job roles to ensure that users have access only to systems and data required for performing their tasks.
- Constantly monitoring privilege accounts to prevent misuse.

■ **Conducting regular security assessments:**

- Conducting vulnerability assessments to scan and plug vulnerabilities before they are exploited.
- Performing regular penetration testing to identify and fix vulnerabilities.
- Ensuring software, applications and operating systems are scanned for updates and patches.

■ **Securing the network perimeter:**

- Using firewalls to block unauthorised access.
- Monitoring network traffic for suspicious activities and preventing intrusions by implementing Intrusion Detection & Prevention Systems
- Securing remote access to the network through Virtual Private Networks (VPNs) and encrypting communications.

■ **Protecting data from unauthorised access:**

- Encrypting data stored on servers, databases, other storage devices

and data in transit to prevent unauthorized access.

- Implementing data loss prevention (DLP) solutions to prevent unauthorized transmission of sensitive data.
- Maintaining regular back up of critical data and regular testing of disaster recovery plans.

■ **Enabling endpoint and device security:**

- Installing and regularly updating antivirus and anti-malware software on all endpoint devices such as computers, mobile devices and servers.
- Securing and managing mobile devices used by employees to ensure they meet security standards.

■ **Implementing a robust incident response plan:**

- Establishing a team of experts for handling breaches and security incidents.
- Creating a detailed incident response plan defining the steps to be taken in the event of a cyber incident.
- Recording learning from the incidents post addressing the security concerns.

■ **Assessing third party risks:**

- Ensuring third party service providers adhere to the security standards.
- Including cybersecurity clauses in contracts with vendors to ensure compliance with data protection regulations and security requirements.

■ **Employee training and awareness:**

- Educating employees on cybersecurity best practices, identification

on phishing emails, social engineering attacks etc.,

- Encouraging employees to report suspicious activities and security threat incidents.
- Sensitize employees on collection, storing and sharing sensitive personal data.

■ **Red teaming and blue teaming:**

- Simulating real-world attacks by having red teams perform adversarial testing to identify weakness in the systems.
- Enhancing the organization's ability to detect and respond to attacks by continuously improving monitoring and incident response capabilities.

■ **Conducting regular security audits:**

- Conducting regular compliance audits to ensure that applicable regulations on cybersecurity and data privacy are complied with.
- Enabling necessary tools for logging security incidents on real time basis for quick detection and remediation.

■ **Continuous monitoring:**

- Enabling necessary tools for logging security incidents on real time basis for quick detection and remediation.
- Leveraging threat intelligence to stay updated on emerging threats, vulnerabilities, and attacker tactics.

Conclusion

Understanding the risks in the Digital Era and mapping out a strategy to ensure that IT controls are in place is a crucial step for businesses where internal audit can play a significant role. The effectiveness of internal audit itself can be enhanced with the use of technology and tools.

Writing Effective Internal Audit Reports – An Art

“The most important thing in communication is hearing what isn't said.”

– Peter Drucker

Internal audits assess organization's internal controls, risk management processes, and operational efficiency. Internal auditors give useful insights and recommendations for improvement by conducting various types of audits, including financial, operational, compliance, information systems, risk management, fraud, governance, and environmental audits.



The audit report is the end result of an audit and should be capable of being used by the recipients as a tool for making decisions. An effective audit report is essential to making sure the results of the audit are presented in a way that is useful to the party receiving the audit.

An internal audit report is a formal document that summarizes the findings of the audit conducted often reflecting on company's financial performance, financial reporting, level of compliances (both internal as well as with regulations), risk management, corporate governance, etc.

In the past, an audit report could afford to be a dry recount of findings and were mere checklists of procedural adherence. As the landscape of governance, risk management, and compliance has evolved, so is internal audit reports.

In our current climate, the internal audit report has become a powerful tool for driving change, identifying risks, and enhancing governance frameworks. In contemporary world, internal audit reports are sophisticated narratives that capture the essence of an organization's health, providing actionable insights that can help enhance the control environment in a march towards being more risk resilient.

It must be remembered that even the most profound insights can fall flat if not communicated effectively. The value of clarity and simplicity in communication cannot be overstated.

In this section we attempt to provide a guide to walk you through the art and science of crafting these reports, ensuring they are effective, hitting the right cords, enhancing readability.

We hope that this guide will demonstrate sound practices for writing internal audit reports that are clear, concise, and actionable.

8.1 Overall process of internal audit report



8.2 Understand objectives and scope of audit

Before getting into the specifics of writing an audit report, it is important to have a broad view of the major objectives of all audit reports. Some of the aspects to be considered area;

- Why was the audit conducted?
- What was included and not included in the audit?
- What was the time period audited?
- What were the broad audit objectives?

8.3 Understanding Audience

An effective audit report begins with a deep understanding of audience. Different stakeholders have varied needs and therefore the report should be able to cater to all those needs:

- **Audit Committee, Board & Senior Management:** They require a very high-level summary that focus on significant risks and their potential impact on the organization. Therefore report should answer few critical questions such as:
 - What's wrong?
 - What is the impact? Financial or otherwise.
 - Practical, long term and affordable solutions
 - A clear action plan and way forward

The report to the highest body should avoid overwhelming them with unnecessary details and instead provide clear, actionable information.

- **Process Owners:** They require detailed, actionable recommendations that address specific operational risks. The content should focus on causes and risks, supported by a summary of the conditions found during the audit. Recommendations should be practical and tailored to the operational context.
- **External Stakeholders:** The needs of external stakeholders, such as regulators or donors, can vary. Reports should provide appropriate context and be tailored to the specific requirements of these audiences, ensuring that the information is thorough yet concise.

8.4 Writing philosophies

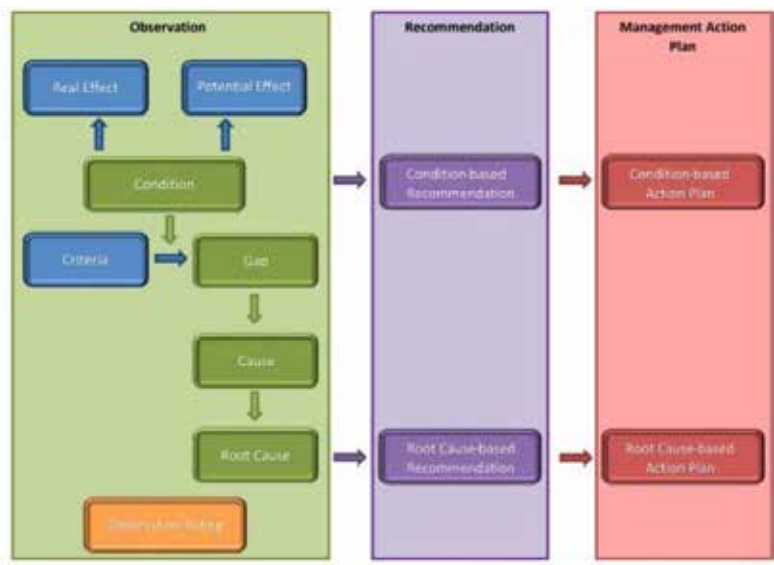
To enhance the quality of audit reports, following writing techniques are important:

- **Simplicity and Clarity:** Express ideas using small, simple words. Avoid legalese or overly complex language. The reports should be easy to read and understood. Minimise use of technical jargon to ensure that the report is accessible to all readers, regardless of their technical expertise.
- **Prioritise Important Findings:** The report should ensure that the most critical information stands out. Through the effective use of headings, subheadings and visual elements like charts and tables to draw attention to key points. This structure helps busy executives quickly find and absorb the information they need.
- **Reporting Protocol:** The report should maintain an objective language tone without any bias or subjectivity.
- **Positive Reinforcement:** Acknowledge areas where management has performed well. This can help foster a cooperative relationship and encourage continuous improvement.
- **Be precise:** it is important to avoid redundant phrases and sentences. Shorter write up with focussed attention is always welcomed by the readers.

8.5 Presentation and Structure

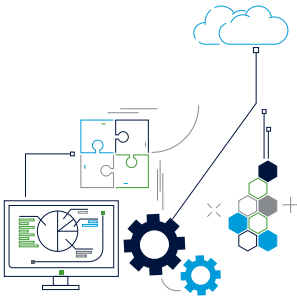
The presentation of information in the report can significantly impact its effectiveness and therefore it is the most critical aspect to be kept in mind while drafting the report. An overall summary of contents is depicted as under:

Source: Institute of Internal Auditors



8.6 Following are important aspects for report presentation:

- **Visual Aids:** Use charts, graphs, and tables to enhance understanding. These elements can make complex data more accessible and highlight key findings.
- **Appendices and Supporting Documents:** Include detailed technical information in appendices to keep the main report focused on critical findings and recommendations. This approach ensures that the core report remains concise and accessible.
- **Tailored Communication:** Customize the report's content and structure to meet the specific needs of each audience, ensuring that the
- **Improvement Areas:** The report should also highlight areas of Improvement wherever possible.



- **Outline audit report:** it is important to make an outline for report based on all the sections of the report. A standard outline is comprised of headings, marked by Numerals, subsections that use letters, numbers, or lowercase, etc.
- **Executive Summary:** The executive summary provides an overview of the audit results.
- **Structure of detailed report:** The detailed report should be carefully drafted and following aspects should be considered:
 - **Audit Scope & Objectives:** the report should clearly define the goals of the audit and the areas covered. The scope should detail what the audit covered, any limitations, and areas not addressed to manage reader expectations.
 - **Background Information:** The objective of providing the Background information is to give the adequate context of the Audit area.
 - **Relevance:** Focus on information that directly impacts the organization's goals. Eliminate any extraneous details that could distract from the core messages of the report.
 - **Root Cause Analysis:** Differentiate between failures in process design and execution, addressing systemic issues. This helps create actionable recommendations that target the underlying problems rather than just the symptoms.
 - **Impact analysis:** the impact of audit findings, financial or otherwise should be clearly stated for each finding so as to understand the value consideration. Without the impact, the audit finding loses its importance. Further the impact



analysis also helps in calibrating audit committee presentations.

- **Risk grading** – each audit findings should be categorised based on its risk grading considering the risks involved, impact, etc. The senior management and the audit committees are more confined to audit findings with very high level of risks and its impact.
 - **Make effective recommendations:** As an auditor, the final task is making recommendations for improvement for the areas audited. Some of the guiding factors are:
 - Be clear as to what specific aspects constitute inconformity and what concrete steps could be potentially implemented to ensure compliance.
 - Identify who should act and make it clear as to who needs to make changes
 - Keep recommendations brief to only include details that are necessary to your point
 - Provide specific, practical recommendations with timelines for implementation. Structure recommendations effectively to ensure that these are persuasive and focused on driving change.
 - Implementation Status of past recommendations are important to understand the acceptability and actions taken by the organisation and often viewed very critical by the Board/Audit Committees. This section should give clarity of what is implemented, what actions are still pending and how the organisation plans to implement it with revised timelines, if any.
- **Quality check and review:** it is always prudent to perform quality checks and get the contents of the audit report review and vetted, ideally by

someone who does not have direct involvement with the audit. This will help in bringing in a “fresh eyes” perspective to the report.

- **Review and proofread:** Before finishing the report, thoroughly review and proofread it. Look for grammatical errors, typos, and inconsistencies in the content. Check that the report respects the appropriate formatting rules and, if relevant, the organization's style guide.
- **Distribution of reports:** The reports should be communicated according to the agreed communication plan. Timely communication allows management to take appropriate corrective and preventive action. To ensure timely communication of engagement results and execution of internal audit plans, a good practice is to issue the draft report within a few days of the exit meetings and the final written report within two weeks of the draft. The written internal audit report should be issued in a timely manner after the conclusion of the internal audit engagement and should not contain any surprises.

8.7 Process of issuance of audit report

While each organisation may lay down its own processes for audit reports, ideal and widely used process includes:

- **Discussion draft report:** this is prepared immediately upon conclusion of audit field work. It helps in ideating the audit findings and should be shared with the process owners/auditees upon closure of field work
- **Report discussions / exit meetings:** this should be planned based on above draft issued to the process owners
- **Formal draft report:** this is prepared post exit meeting with process owners and can account for changes upon receiving initial feedback and response from the auditees.
- **Final report:** this is issued post receiving formal responses from auditees as to audit findings, recommendations, action plans, timelines for

implementation, etc.

8.8 Expectations of Stakeholders from the Internal Audit Report

- **Clarity and Conciseness:** The report should be well-structured, clearly communicating key findings, risks, and recommendations. It should avoid unnecessary jargon and excessive detail, focusing on material issues.
- **Actionable Recommendations:** The report should provide practical, specific, and prioritized recommendations that management can implement to address identified risks and enhance internal controls, processes, and compliance.
- **Risk-Based Insights:** The report should identify critical risks (financial, operational, compliance, or strategic) and their potential impact on the organization's objectives. It should also assess the effectiveness of existing risk mitigation measures.
- **Management's Response and Action Plan:** The report should include management's response to the audit findings, along with a timeline and accountability for implementing corrective actions, ensuring follow-up and closure.
- **Alignment with Strategic Objectives:** The report should ensure that the internal audit findings align with the organization's overall strategic goals, corporate governance, and regulatory requirements, while also highlighting emerging risks and trends.

Conclusion

By applying above guidelines, the Internal Audit Department can produce reports that are not only clear and concise but also impactful and actionable. The ultimate goal is to deliver information that helps the organization achieve its objectives while maintaining strong relationships with management and other stakeholders.

Bibliography

AAA: Analytics, Automation and Artificial Intelligence

ACB: Audit Committee Board

AI: Artificial Intelligence

BYOD: Bring Your Own Device

CCPA: Central Consumer Protection Authority

CEO: Chief Executive Officer

CSR: Corporate Social Responsibility

CRM: Customer Relationship Management

DA: Data Analytics

DLP: Data Loss Prevention

DPDPA: Digital Personal Data Protection Act

ESG: Environmental, Social, and Governance

ERM: Enterprise Risk Management

ERPs: Enterprise Resource Planning Systems

GDPR: General Data Protection Regulation

GRC: Governance, Risk and Control

HIA: Head of Internal Audit

HIPAA: Health Insurance Portability and Accountability Act

IAM: Identity Access Management

IA: Internal Audit

IASB: Internal Audit Standards Board

ICAI: Institute of Chartered Accountants of India

ICF: Internal Control Framework

IIA: Institute of Internal Auditors

IPPF: International Standards for the Professional Practice of Internal Auditing

KPI: Key Performance Indicators

ML: Machine Learning

RBIA: Risk Based Internal Audit

RPA: Robotic Process Automation

SIA: Standards on Internal Audit

SLA: Service Level Agreement

SME: Subject Matter Experts

SOD: Segregation of Duties

SQL: Structured Query Language

TVM: Threat and Vulnerability Management

WTD: Whole Time Director

[illegible]

[illegible]

NOTES

**Mumbai (Corporate Office)**

8th floor, Bakhtawar
229, Nariman Point
Mumbai – 400 021

3rd floor, Technopolis Knowledge
Park, A Wing, MIDC
Andheri East, Mumbai – 400 093

Navi Mumbai

1201A, Rupa Renaissance
Juinagar, MIDC Road
Navi Mumbai – 400 705

New Delhi – NCR

2nd & 3rd floor, B37, Sector 1
Noida – 201 301

Chennai

2nd & 4th floor, Apex Towers
R.A. Puram, Chennai – 600 028

Bengaluru

3rd floor, Jubilee Building
45, Museum Road
Bengaluru – 560 025

Hyderabad

301, Block-1, White House
Greenlands Road Kundanbagh
Begumpet, Hyderabad – 500 016

Kolkata

5th floor, J K Millennium Centre
Jawaharlal Nehru Road
Kolkata – 700 071

Surat

RSM House, DTA-2
G-02 to G-05 Plot
Gujarat Hira Bourse
Ichhapore-2, Surat – 394 510

Ahmedabad

B/211, 2nd floor, Mondeal Heights
Opp. Karnavati Club, S.G. Highway
Ahmedabad – 380 015

Pune

603, Pride House
Ganesh Khind Road
Opp. NIC University Chowk
Pune – 411 016

Gandhidham

206, Sunshine Arcade II
Plot No. 37, Sector 8
Near D-Mart
Gandhidham – 370 201

Jaipur

346, 3rd floor, Ganpati Plaza
M.I. Road, Jaipur – 302 001

Vijayanagar

A2/UT-F, Power Valley
JSW Steel Township Toranagullu
Bellary – 583 123

For further information please contact:

RSM Astute Consulting Pvt. Ltd.

8th Floor, Bakhtawar, 229, Nariman Point, Mumbai – 400021.

T: (91-22) 6108 5555/ 6121 4444

F: (91-22) 6108 5556/ 2287 5771

E: emails@rsmindia.in **W:** www.rsmindia.in

Offices: Mumbai, New Delhi – NCR, Chennai, Kolkata, Bengaluru, Navi Mumbai, Surat, Hyderabad, Ahmedabad, Pune, Gandhidham, Jaipur and Vijayanagar.



facebook.com/RSMInIndia



twitter.com/RSM_India



linkedin.com/company/rsm-india



Youtube.com/c/RSMIndia

RSM Astute Consulting Pvt. Ltd. (including its affiliates) is a member of the RSM network and trades as RSM. RSM is the trading name used by the members of the RSM network.

Each member of the RSM network is an independent accounting and consulting firm each of which practices in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction.

The RSM network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 50 Cannon Street, London EC4N 6JJ.

The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

This Publication provides an overview of various aspects of Internal Audit. It may be noted that nothing contained in this Publication should be regarded as our opinion and facts of each case will need to be analyzed to ascertain thereof and appropriate professional advice should be sought for applicability of legal provisions based on specific facts. We are not responsible for any liability arising from any statements or errors contained in this Publication.

This Publication is protected under Copyright and Intellectual property laws and regulations.

January 2025

© RSM India, 2025