

Publication – Internal Audit in BFSI Sector:
Leveraging Automation, Analytics
and Artificial Intelligence



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 14 key cities across India
- Multi-disciplinary personnel strength of over 3,000
- International delivery capabilities

[rsmindia.in](https://www.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\$ 10 billion
- Combined staff of over 65,000 in over 900 offices across more than 120 countries

[rsm.global](https://www.rsm.global)



Table of Contents

Sr. No.	Particulars	Page No.
	Preface	1
1.0	Role of Internal Audit and Risk Management in the BFSI Sector	2
2.0	Automation, Analytics and Artificial Intelligence (AAA) in Internal Audits	5
2.1	Data Analytics Enabled Automation	5
2.2	Artificial Intelligence in Internal Audit	9
2.3	Tools deployed for analytics and automation in Internal Audit	16
2.4	Auditing in an AI Environment	17
2.5	Technology Impact and Changing Dynamics of Internal Audit	18
2.6	Information Technology in Internal Audit – A Key Differentiator	19
2.7	Digital Personal Data Protection Act, 2023	31
2.8	Conclusion	41
3.0	Cybersecurity – Key Aspects for Consideration	42
3.1	Need for Cybersecurity	42
3.2	Cybersecurity Landscape and Cyber Threats	42
3.3	Cyber Security Landscape	43
3.4	Major Cyber Threats	43
3.5	Regulatory Bodies and Policy Frameworks	47
3.6	Regulatory Bodies	48
3.7	Indian Computer Emergency Response Team (CERT-In)	49
3.8	National Critical Information Infrastructure Protection Centre (NCIIPC)	50
3.9	National Cyber Coordination Centre (NCCC)	50
3.10	Reserve Bank of India (RBI)	51
3.11	Telecom Regulatory Authority of India (TRAI)	52
3.12	Policy Frameworks	52
3.13	National Cybersecurity Policy, 2013	53
3.14	Information Technology Act, 2000	55
3.15	National Cybersecurity Strategy, 2020	58

Table of Contents

Sr. No.	Particulars	Page No.
3.16	Strategic Actions and Initiatives	59
3.17	Challenges in Cybersecurity	61
3.18	Enhancing Cybersecurity Posture	61
3.19	Conclusion	64
4.0	Internal Audit Standards – An Overview	66
4.1	Standards on Internal Audit (Global and ICAI Pronouncements)	66
4.2	Global Standards: The IPPF Framework	67
4.3	ICAI's Standards on Internal Audit (SIAs)	68
5.0	BFSI Segments and Potential Value Additions by Internal Audit	78
5.1	Banking Sector	78
5.2	Insurance Sector	91
5.3	Depository Participant	108
5.4	Wealth Management	114
5.5	Asset Management	120
5.6	Retail and Institutional Broking	124
5.7	Investment Banking	127
5.8	Fintech Platforms	129

PREFACE

- Banking, Financial Services and Insurance (BFSI) sector in India has witnessed a meteoric growth in the last few years and is set to grow exponentially due to rising per capita income, introduction of new products, innovation in technology, expanding distribution networking and increasing customer awareness of financial products.
- BFSI in India has earned a reputation to stand out in the global financial turmoil and geo-political upheavals due to its strong regulatory and compliance framework and robust monetary policies.
- Economic expansion of Indian markets due to higher GDP growth rates in the past and forecast for a sustainable economic growth in future years will require a stronger BFSI sector.
- **Important regulators in the BFSI sector include:**
 - Reserve Bank of India (Banking)
 - Securities & Exchange Board of India (Financial Services)
 - Insurance Regulatory Development Authority (Insurance)
 - Pension Funds Regulatory Development Authority (Pension Funds)
- The role of Automation, Analytics and Artificial Intelligence (AAA) will be very critical for organizations to stay resilient and adaptable in a fast-evolving business environment.
- This booklet is intended to provide an insight into the role of Internal Audit and Risk Advisory in the BFSI sector. The booklet is not intended to be a comprehensive document but rather to reflect the emerging trends and the changing role of Internal Audit and Risk Management in the context of the BFSI sector.

Chapter 1 Role of Internal Audit and Risk Management in the BFSI Sector

1.1 Internal Audit & Risk Management in the BFSI sector is primarily intended to provide the management with a clear, comprehensive and unbiased analysis of the adequacy, existence and effectiveness of internal controls and risk management framework of the entity. It reviews the functional efficiency of the organization with a view to suggesting areas for possible improvements.



It is an important tool which enables an organization in achieving its strategic business goals, meet operational and business environmental challenges, comply with regulatory norms and managing reporting requirements.

1.2 Internal Audit includes:

- Critical evaluation of internal controls, performing GAP analysis & suggesting areas for strengthening;
- Constructive review of business operations by keeping the organisation's business needs in focus;
- Identification & recommendation of areas for cost reduction, revenue optimization & improvement in operational efficiency;
- Critical evaluation of systems & procedures and adherence to SOPs;
- Review of Information Technology (IT) controls and Business Continuity Plan
- Identification, assessments & control of risks;
- Review of compliances with the various regulatory provisions & operations manuals;
- Review of adherence to the corporate governance requirements

1.3 As per the Institute of Internal Auditors "Enterprise-wide Risk Management (ERM) is a structured, consistent and continuous process across the whole organization for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives". The responsibility of

ERM is with the Board.

1.4 Internal audit is an independent, objective assurance activity and can provide valuable insight in providing assurance that major business risks are being managed appropriately and the risk management and internal control framework is operating effectively.

1.5 ERM role shall include the following:

- Facilitating identification and evaluation of key risks
- Evaluating and reporting of key risks
- Consolidating risks across the organization
- Developing and maintaining the ERM framework

However, internal audit should not be involved in setting risk appetite, taking decision on risk response, implementing risk response or taking accountability of risk management.

1.6 Internal Audit's core role in relation to ERM should be providing assurance to management and to the Board on the effectiveness of risk management.

1.7 Internal Audit & Risk Management in today's global competitive environments depends heavily on Information Systems for decision making. Business processes are increasingly getting automated and controls are becoming less person-dependent. In such a scenario, the significance of Information Technology (IT) & Information Systems (IS) cannot be undermined as these are pervasive throughout the business.

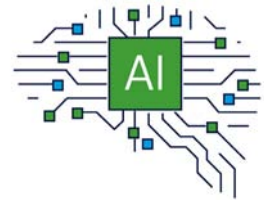
1.8 Current Trends in Internal Audit include:

- **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.
- **Modern Auditing techniques:** Data Analytics (DA) and continuous auditing have really changed how internal audits work nowadays. Frameworks like the Internal Control Framework (ICF) and the 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.

- **Data-driven decision-making:** This 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.
- **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.
- **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.
- **Operational Audit:** The evolution of IA paved the way for management and operational audits.
- **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.
- **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.
- **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.

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.

2.1 Data Analytics Enabled Automation

2.1.1 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 control.

2.1.2 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.

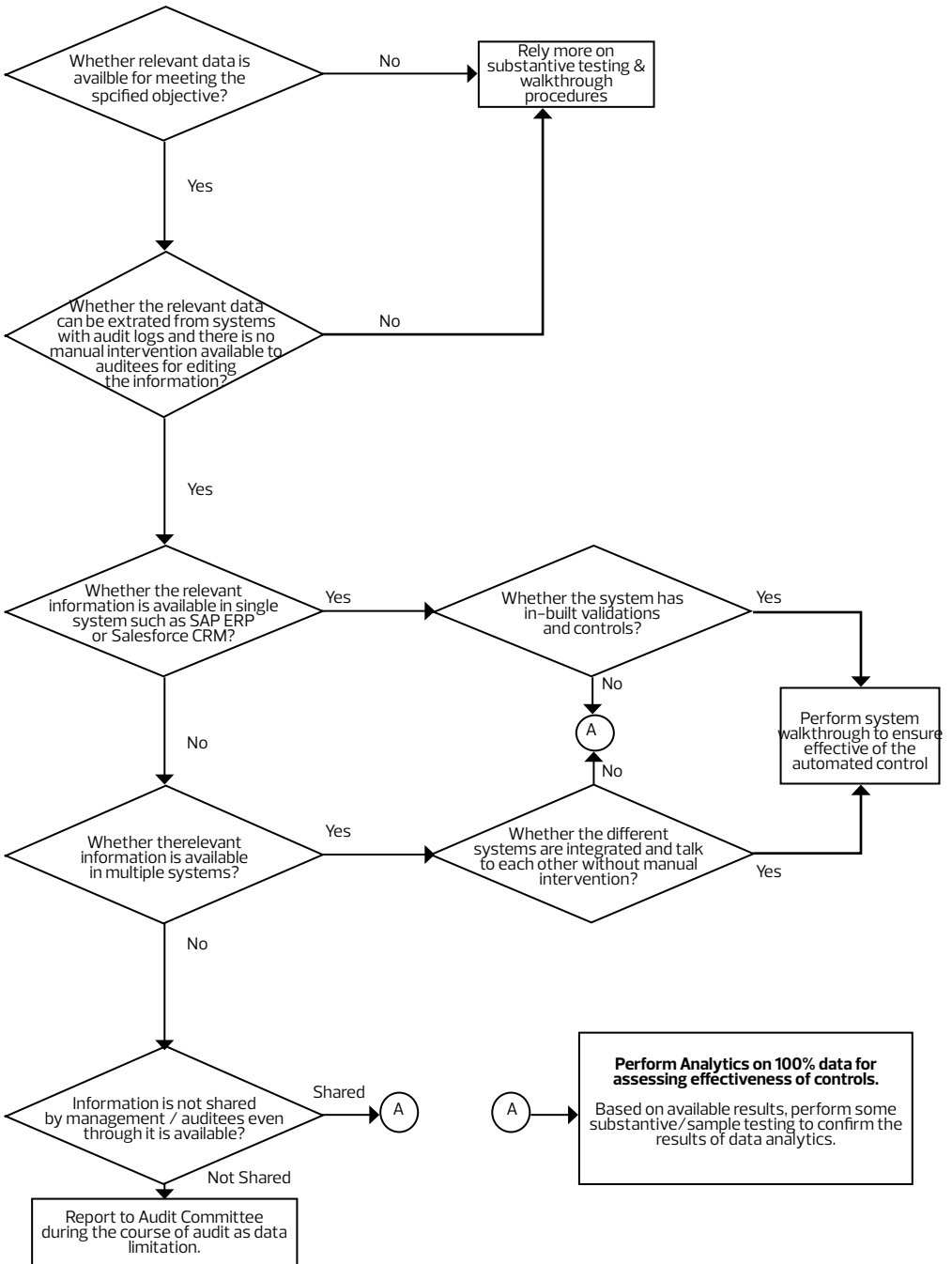
2.1.3 Why is Data Analytics used in Internal Audits?

- **Data Analytics is an indispensable part of internal audits:** It is a given fact that if internal audit has to provide assurance on the 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 the effectiveness of internal controls.. 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 analyzing 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.

2.1.4 When can Data Analytics 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, the following are the factors that determine the usage of data analytics in internal audits:
 - a) **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 manner – for example, if there is text captured, the same is generally done in a predefined manner.
 - b) **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 generates a lot of value for the company and management.

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



2.1.5 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 the emergence of analytical tools (refer to 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 a number of specialized computing systems for different aspects of business environments, internal auditing will continue to rely on data analytics for times to come.

2.2 Artificial Intelligence in Internal Audit

2.2.1 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.

Generative AI, the game changer: The recent emergence of generative AI has

been game changing not only for the 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 a fast pace, and there are new fields and a huge number of organizations developing AI platforms, with both narrow and broad capabilities.

2.2.2 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.*”

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

2.2.3 How can Generative AI be used in Internal Audits?

Risk assessment	Audit plan development	Engagement planning	Execution	Reporting
<ul style="list-style-type: none"> Supporting auditor research and understanding of risk for a specific industry Supporting audit universe creation e.g. guidance on universe design, process universe, etc. 	<ul style="list-style-type: none"> Supporting auditor research and understanding on risk, business process and expected controls in advance of engagement planning Suggested audits against the risk assessed 	<ul style="list-style-type: none"> Suggest test procedures based on in scope risk areas Suggest data sources, tables and potential analytics tests Generate scripts for data extract and analytics execution 	<ul style="list-style-type: none"> Analysis of data through natural language questioning Suggested interview questions for different stakeholders Critical assessment of risk and control descriptions (e.g. if it covers 	<ul style="list-style-type: none"> Initial draft report Editorial QA e.g. simplifying language, sentiment analysis Preparation of reports for Audit Committee summaries Generation of video/ audio reporting Customised

Risk assessment	Audit plan development	Engagement planning	Execution	Reporting
	audit universe <ul style="list-style-type: none"> Suggested scheduling and resource allocation based on known constraints e.g. number and levels of staff 	<ul style="list-style-type: none"> First draft of scope/terms of reference 	who, what, where, when, etc.) <ul style="list-style-type: none"> Initial draft of workpaper Drawing themes from interview notes Summation / interrogation of audit evidence documents Initial workpaper review and QA Initial draft of observations. 	communications stakeholders' style <ul style="list-style-type: none"> Drafting emails to communicate the audit report

2.2.4 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 the 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:

- Attendance and leaves information comes from Biometric and an excel extract is passed on as input to the payroll team for processing.
- 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:

Suggested Control Tests

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 Joinees 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 all 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:

C:\Users\pariharm\OneDrive - Suresh Surana & Associates LLP\12.

UrbanL\3. RSM Workings\00. Mohit\Vendor Master-combined.xlsx

Sheet name = vendorMaster.

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 save a significant amount of time and also empower 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:

```
python Copy code
import pandas as pd
from fuzzywuzzy import fuzz
```

```

# Load the vendor master data from Excel
input_path = r"C:\Users\pariharm\OneDrive - Suresh Surana & Associates LLP\12. UrbanL\3. R
df = pd.read_excel(input_path, sheet_name='vendorMaster')

# Add an empty 'Name_match' column
df['Name_match'] = ''

# Define a fuzzy matching function for names
def fuzzy_match_names(row):
    if pd.isnull(row['Name']) or pd.isnull(row['Name_match']):
        return False
    return fuzz.ratio(str(row['Name']), str(row['Name_match'])) <= 50

# Case a: Duplicate vendor names with fuzzy matching ratio more than 80% within the same c
duplicate_names = df[df.duplicated(['Name', 'City'], keep=False)]
df['Fuzzy Match'] = duplicate_names.apply(lambda row: fuzz.ratio(str(row['Name']), str(row

# Case b: PAN not updated
pan_not_updated = df[df['P.A.N. No.'].isnull()]

# Case c: Vendors having the same PAN but different names
duplicate_pans = df[df.duplicated('P.A.N. No.', keep=False)]
df.loc[duplicate_pans.groupby('P.A.N. No.').head(1).index, 'Name_match'] = duplicate_pans.
same_pans_diff_names = duplicate_pans[duplicate_pans.apply(fuzzy_match_names, axis=1)]

# Case d: GST No. not updated
gst_not_updated = df[df['GST Registration No.'].isnull()]

# Case e: Same Bank A/c mapped to multiple vendors with different names
duplicate_accounts = df[df.duplicated('Bank Account Number', keep=False)]
df.loc[duplicate_accounts.groupby('Bank Account Number').head(1).index, 'Name_match'] = du
same_accounts_diff_names = duplicate_accounts[duplicate_accounts.apply(fuzzy_match_names,

```

2.2.5 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.

2.2.6 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 that choose to ignore these technologies will fall behind, but their adoption of them must be managed and considered. **The 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 skepticism
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 for human involvement.
Data security loss: Sensitive or confidential information could inadvertently leave the organization when 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.
Bias Propagation: Gen AI can perpetuate and even amplify existing biases in the data they were trained on.	Maintain a healthy level of professional skepticism.

2.2.7 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.

2.3 Tools deployed for analytics and automation in Internal Audit

Internal Auditors generally deploy the following tools for data analytics and automation:

<p>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.</p> 	<p>Data Visualization Tools: These tools are used to create interactive dashboards and visualizations, enabling auditors to identify insights and trends quickly.</p> 
<p>Programming Languages / Databases: Python is used for advanced analytics, scripting, and machine learning, while SQL is essential for querying and managing relational databases.</p> 	<p>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.</p> 

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 the 6 different segments mentioned above, Generative AI tools can be used to enhance productivity and creativity in Internal Audits.



ICAI Internal Audit GPT ✓

2.4 Auditing in an AI Environment

2.4.1 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.

2.4.2 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.

2.4.3 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.

2.5 Technology Impact and Changing Dynamics of Internal Audit

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 overrides and the mechanisms for audit trails of such overrides?
- Does your audit plan identify key IT risks that have a direct significant impact on the organization?
- 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?

2.6 Information Technology in Internal Audit – A Key Differentiator

- Internal audits are designed to evaluate the effectiveness an 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 the emerging environment and the requirement to perform audit tasks effectively, auditors must recognise the key reasons to use audit tools and software.
- **Key IT considerations for Internal Audit include the following :**

➤ **Information Security**

Information Security	Key IT Internal Audit Considerations
<p>Information security program assessment – Evaluates the organization's information security program, including strategy, awareness and training, vulnerability assessments, predictive threat models, monitoring, detection and response, technologies and reporting.</p>	<ul style="list-style-type: none"> ● How comprehensive is the existing information security program? ● Is information security embedded within the organization, or is it an "IT only" responsibility? ● How well does the organization self-assess threats and mitigate them? ● How well does the organization finds the vulnerabilities and the solution for that?
<p>Threat and vulnerability management program assessment – Evaluates the organization's Threat and Vulnerability Management (TVM)</p>	<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 organization?

Information Security	Key IT Internal Audit Considerations
<p>program including threat intelligence, vulnerability identification, remediation, detection, response, and countermeasure planning.</p>	<ul style="list-style-type: none"> ● 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 to the TVM?



Business Continuity Management

Business Continuity Management	Key IT Internal Audit Considerations
<p>Business continuity program integration and governance audit – Evaluates the organization'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</p>	<ul style="list-style-type: none"> ● Does a holistic business continuity plan exist for the organization? ● How does the plan compare to leading practice? ● Is the plan tested? ● What impact will the plan have on the business?
<p>Disaster recovery audit – Assesses IT's ability to effectively recover systems and resume regular system performance in the event of a disruption or disaster.</p>	<ul style="list-style-type: none"> ● Are disaster recovery plans aligned with broader business continuity plans? ● Do testing efforts provide confidence that systems can be effectively recovered? ● Are all critical systems included? Are critical systems defined?

Business Continuity Management	Key IT Internal Audit Considerations
<p>Crisis management audit – Reviews the organization's crisis management plans, including overall strategy/plan, asset protection, employee safety, communication methods, public relations, testing, maintenance, change management and training/awareness.</p>	<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?



Mobile Security

Mobile Security	Key IT Internal Audit Considerations
<p>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 accessibility and policy configuration.</p>	<ul style="list-style-type: none"> ● How has the organization 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? ● How do we manage lost and stolen devices? ● What vulnerabilities exist, and how do we manage them?
<p>Mobile application black box assessment – Performs audit using different front-end testing strategies: scan for vulnerabilities</p>	<ul style="list-style-type: none"> ● What vulnerabilities can be successfully exploited? ● How do we respond when exploited, and do we know

Mobile Security	Key IT Internal Audit Considerations
using various tools, and manually verify scan results. Attempts to exploit the vulnerabilities identified in mobile web apps.	an intrusion has occurred?
<p>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.</p>	<ul style="list-style-type: none"> ● How sound is the code associated with the mobile applications used within the organization? ● What vulnerabilities can be exploited within the code? ● Whether OWASP top 10 vulnerabilities are present in the code?
<p>Device Security configuration</p>	<ul style="list-style-type: none"> ● Have your IT servers, infrastructure securely hardened? ● Are the security patches updated appropriately? ● Do you follow leading industry practices to secure systems?



Cloud Security

Cloud Security	Key IT Internal Audit Considerations
<p>Cloud strategy and governance audit – Evaluates the organisation's strategy for utilizing</p>	<ul style="list-style-type: none"> ● Are there supporting policies to follow when using a cloud provider? Are

Cloud Security	Key IT Internal Audit Considerations
<p>cloud technologies. Determines whether the appropriate policies and controls have been developed to support the deployment of the strategy.</p> <p>Evaluates alignment of the strategy to overall company objectives and the level of preparedness to adopt within the organisation.</p>	<p>policies integrated with legal, procurement and IT policies?</p> <ul style="list-style-type: none"> ● How to make the organization to adopt the changes?
<p>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.</p>	<ul style="list-style-type: none"> ● Does your organization have secure authentication protocols for users working in the cloud? ● Have the right safeguards been contractually established with the provider?
<p>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</p>	<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?

Cloud Security	Key IT Internal Audit Considerations
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"> ● Does the organization have an inventory of uses of external cloud service providers, sponsored both within IT and directly by the business units?



Social Media Risk Management

Social Media Risk Management	Key IT Internal Audit Considerations
<p>Social media risk assessment – Collaborates with the IT organization to assess the social media activities that would create the highest level of risk to the organization. Evaluates the threats to the organization'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 organization.</p>	<ul style="list-style-type: none"> ● Has the organization identified what risks exist related to social media? ● How well are the identified risks managed or mitigated? ● Does the organization periodically conduct a social media audit?
<p>Social media governance audit – Evaluates the design of policies and procedures in place to manage social media within the organization. Reviews policies and procedures against leading practices.</p>	<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?
<p>Social media activities audit – Audits the social media activities of the organization and its employees</p>	<ul style="list-style-type: none"> ● Are social media activities aligned to policy? ● What corrective actions

Social Media Risk Management	Key IT Internal Audit Considerations
<p>against the policies and procedures in place. Identifies new risks and assist in developing policies and controls to address the risks.</p>	<p>need to be put in place given activity?</p> <ul style="list-style-type: none"> ● How does existing activity affect brand and reputation?

➤ **Segregation of Duties & Identity Access Management (SoD & IAM)**

SoD & IAM	Key IT Internal Audit Considerations
<p>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 where conflicts exist</p>	<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 detect financial misstatement, would they truly detect fraud?
<p>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.</p>	<ul style="list-style-type: none"> ● Does the organization 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?

SoD & IAM	Key IT Internal Audit Considerations
<p>Segregation of duties remediation audit – Follows up on previously identified external and internal audit findings around SoD conflicts.</p>	<ul style="list-style-type: none"> ● Does the organization take appropriate action when SoD conflicts are identified? ● Have we proactively addressed SoD issues to prevent year-end audit issues?
<p>IAM/GRC technology assessment – Evaluates how IAM or GRC software is currently used, or could be used, to improve SoD controls and processes.</p>	<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?



Data Loss Prevention (DLP) and Privacy

Data Loss Prevention (DLP) and Privacy	Key IT Internal Audit Considerations
<p>Data governance and classification audit – Evaluates the processes management has put in place to classify data, and develops plans to protect the data based on the classification</p>	<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?
<p>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</p>	<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

Data Loss Prevention (DLP) and Privacy	Key IT Internal Audit Considerations
messaging, privileged user monitoring, data sanitation, data redaction, export / save control, endpoint security, physical media control, disposal and destruction, and mobile device protection.	done to manage these gaps?
<p>Privacy regulation audit – Evaluates the privacy regulations that affect the organization, and assess management's response to these regulations through policy development, awareness and control procedures.</p>	<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 organizations, 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?



Machine Learning

Machine Learning in Internal Audit	Key IT Internal Audit Considerations
<p>Machine learning technology helps in finding the unstructured data, which includes the emails and the social media posts and reviews them.</p>	<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?

Machine Learning in Internal Audit	Key IT Internal Audit Considerations
<p>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</p>	<ul style="list-style-type: none"> ● Where is our data going? ● What is the historical transaction pattern? ● How the transactions are classified? ● What are the controls to protect the historical transaction data?
<p>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</p>	<ul style="list-style-type: none"> ● What is the pattern of data being processed? ● What type of algorithms in place for analysis so it meet the requirements? ● Has any feedback mechanism been carried?



Block Chain

Blockchain in Internal Audit	Key IT Internal Audit Considerations
<p>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.</p>	<ul style="list-style-type: none"> ● Whether the Existing policies and procedures will need to be updated to accommodate blockchain protocols and integrate blockchain transactions into legacy systems?
<p>Blockchain technology helps to test the whole population of transactions within the period under observation. This extensive</p>	<ul style="list-style-type: none"> ● What type of data is processed? ● Is the data structured or unstructured?

Blockchain in Internal Audit	Key IT Internal Audit Considerations
<p>coverage will drastically improve the level of assurance gained in affected audit engagements.</p>	<ul style="list-style-type: none"> ● What controls do we have in place to protect data?
<p>Blockchain uses the encryption technology which helps to secure the data.</p>	<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?



Robotics Process Automation

Blockchain in Internal Audit	Key IT Internal Audit Considerations
<p>RPA is configurable software, that works on the existing IT infrastructure, pulling data, performing algorithms, and creating reports. It uses business rules, can be configured to perform a variety of processes enabling multi-use robots, and variability as your business needs change.</p>	<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 organization follow in the context of RPA? ● Have optimized processes before we automated?
<p>RPA offers broader spectrum of internal and external application integration in risk. It help to create document repositories and connections to existing governance, risk and control</p>	<ul style="list-style-type: none"> ● What level of control implemented to organization on the integration of application? ● Do business users understand the access

Blockchain in Internal Audit	Key IT Internal Audit Considerations
(GRC) platforms that are linked to processes, risks and controls to demonstrate framework adherence and evidence traceability.	being assigned to roles they are assigned ownership of?

2.7 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 framework 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. DPDP Rules were notified on 14 November 2025.

2.7.1 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:
 - a. In digital form; or
 - b. In non-digital form and digitized subsequently.
 - c. 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:**
 - a. **Data Fiduciaries:** Individuals or organizations that determine the purpose and means of processing personal data.
 - b. **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:

- a. The Data Principal to whom such personal data relates; or
 - b. 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.

2.7.2 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.

2.7.3 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.

2.7.4 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 a Data Fiduciary.
- **Data Fiduciaries can process the personal data of Data Principal only when:**
 - Data Principal has given consent or
 - Data processing is covered under “Certain legitimate uses”.

2.7.5 Consent Mechanism :

For obtaining the consent from the 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.

2.7.6 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 itemized description of personal data, specified purpose of, and an itemized 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 a 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 an identify issued by Central / State Government or entrusted by law?

2.7.7 Change / withdrawal of consent:

- Right to manage, review or withdraw the consent with the same ease as 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.

2.7.8 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 an epidemic or any other threats to public health.
- For safety during a 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.**

2.7.9 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.

2.7.10 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:

Sr. 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 the processing of personal data of children	May extend to two hundred crore rupees.
4	Breach in observance of additional obligations of a 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.

2.7.11 Sectors which may be heavily impacted due to the 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

2.7.12 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. **The 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 backup 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 detailing 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 of 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 weaknesses 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.

2.7.13 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 the internal audit itself can be enhanced with the use of technology and tools.

2.8 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 skepticism 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.

Cybersecurity is the comprehensive practice of protecting systems, networks, and data from digital attacks, unauthorized access, and damage, through the implementation of advanced technologies, rigorous processes, and trained personnel, ensuring the integrity, confidentiality, and availability of information in an increasingly interconnected world.

India's digital transformation has been marked by significant initiatives such as Digital India, Smart Cities Mission, and widespread adoption of digital payment systems. As the country embraces these technological advancements, the importance of robust cybersecurity measures becomes paramount. Cybersecurity threats pose risks to national security, economic stability, and individual privacy.

In an era where digital transformation drives every facet of modern society, cybersecurity emerges as a critical pillar safeguarding our interconnected ecosystem. It transcends mere technical measures, evolving into a multidimensional discipline that encompasses a blend of technology, policy, and human behaviour. The relentless advancement of cyber threats—from sophisticated state-sponsored attacks to pervasive ransomware necessitates a proactive and adaptive approach to security. Cybersecurity not only defends against breaches and data theft but also fortifies trust in the digital infrastructure that underpins global commerce, communication, and governance. This dynamic field demands continuous innovation and collaboration to anticipate and counteract the evolving tactics of cyber adversaries, ensuring a resilient and secure digital future.

3.1 Need for Cybersecurity

The rapid digitization of India has catalyzed unprecedented economic growth and improved access to services. However, it has also expanded the country's vulnerability to cyber threats. This paper examines the current cybersecurity landscape in India, identifies the major challenges, and proposes strategic imperatives to strengthen cybersecurity infrastructure.

3.2 Cybersecurity Landscape and Cyber Threats

The cybersecurity landscape denotes the dynamic and multifaceted environment encompassing the various elements, actors, and factors that influence the

security of digital systems and data. It is characterized by a continuous evolution of threats, technological advancements, and regulatory developments. This landscape includes a broad spectrum of components such as threat actors (hackers, cybercriminals, nation-states), types of cyber threats (malware, ransomware, phishing, DDoS attacks), and the defensive measures deployed (firewalls, encryption, intrusion detection systems).

3.3 Cyber Security Landscape

Within the cybersecurity landscape, the interplay between offensive and defensive strategies shapes the overall security posture. Cybersecurity professionals must navigate an ever-changing terrain where new vulnerabilities emerge as technology evolves, requiring constant vigilance, innovation, and adaptation. Moreover, the cybersecurity landscape is influenced by geopolitical dynamics, with cyber warfare and espionage becoming critical elements of national security strategies.

Additionally, the landscape is marked by regulatory and compliance requirements that vary across regions and industries, necessitating a deep understanding of legal frameworks and standards. Organizations must not only defend against attacks but also ensure compliance with regulations such as GDPR, HIPAA, and national cybersecurity policies. In essence, the cybersecurity landscape is a complex and ever-shifting domain that demands a holistic approach, integrating technology, policy, and human factors to protect against the myriad of evolving cyber threats.

3.4 Major Cyber Threats

Cyber threats are malicious activities or actions aimed at exploiting vulnerabilities in digital systems, networks, and devices to cause harm, disrupt operations, steal data, or gain unauthorized access. These threats are perpetuated by various actors, including cybercriminals, hackers, state-sponsored entities, and insider threats, each with distinct motives ranging from financial gain and political agendas to personal vendettas and corporate espionage.

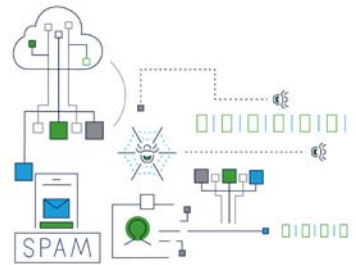
Cyber threats are diverse and constantly evolving, posing significant risks

to individuals, organizations, and nations. Enhancing cybersecurity posture requires a multifaceted approach that includes robust technological solutions, comprehensive policies, continuous monitoring, and ongoing education and training. By understanding and mitigating these major cyber threats, stakeholders can better protect their digital assets and ensure the security and resilience of their operations in the digital age.

3.4.1 Malware and Ransom Attacks

Malware or malicious software, encompasses various types of harmful software, including viruses, worms, trojans, ransomware, and spyware. Malware infiltrates systems to steal, encrypt, or delete sensitive data, disrupt operations, or gain unauthorized access to networks.

- **Ransomware:** Encrypts data and demands a ransom for decryption of data.
- **Spyware:** Secretly monitors users and gathers personal information.
- **Mitigation:**
 - Use reputable antivirus and anti-malware software.
 - Update all systems and software with the latest patches.
 - Educate users on recognizing and avoiding phishing emails and suspicious downloads.



3.4.2 Phishing and Social Engineering

Cybercriminals exploit human psychology to deceive individuals into revealing personal information, leading to identity theft and financial losses. Phishing attacks involve cybercriminals sending deceptive emails or messages designed to trick recipients into revealing sensitive information, such as login credentials, financial information, or personal data. These attacks often mimic legitimate communications from trusted sources.

- **Email Phishing:** Fraudulent emails that appear to come from a trusted organization.
- **Spear Phishing:** Phishing attacks targeted at specific individuals or organizations.
- **Mitigation:**
 - Implement email filtering solutions to detect phishing emails and take necessary action.
 - Conduct regular training sessions for employees on identifying phishing attempts.
 - Use multi-factor authentication (MFA) for additional security.

3.4.3 Distributed Denial-of-Service (DDoS) Attacks

DDoS attacks aim to overwhelm a network, server, or website with a flood of traffic, rendering it inaccessible to legitimate users. DDoS disrupts business operations and causes significant financial losses.

- **Volume-Based Attacks:** Overwhelm the target with massive amounts of data.
- **Application Layer Attacks:** Target specific applications or services, exhausting their resources.
- **Mitigation:**
 - Use DDoS protection services and solutions.
 - Implement a robust network architecture with load balancing and redundancy.
 - Monitor network traffic for signs of unusual activity.

3.4.4 Advanced Persistent Threats (APTs)

APTs are prolonged and targeted cyber-attacks aimed at stealing sensitive

information or compromising critical systems. These attacks are often carried out by well-funded and skilled adversaries, including nation-state actors.

- **Stuxnet:** A highly sophisticated worm that targeted Iran's nuclear facilities.
- **APT10:** A Chinese hacking group known for targeting intellectual property and sensitive data.
- **Mitigation:**
 - Employ advanced threat detection and quick response.
 - Conduct regular security audits and vulnerability assessments.
 - Implement strict access controls and monitor for anomalous activities.

3.4.5 IoT Vulnerabilities

The Internet of Things (IoT) devices have introduced new vulnerabilities that lack robust security features:

- **Mirai Botnet:** Compromised IoT devices to launch large-scale DDoS attacks.
- **Smart Home Hacks:** Exploiting vulnerabilities in smart home devices to gain unauthorized access.
- **Mitigation:**
 - Ensure the devices are updated with the latest firmware and security patches.
 - Use strong passwords for IoT devices.
 - Segment / isolate IoT devices from critical systems by providing separate network.

3.4.6 Cryptojacking

Cryptojacking involves cybercriminals hijacking a target's computational resources to mine cryptocurrencies without their knowledge or consent. This can lead to decreased performance and increased operational costs.

- **Web-Based Cryptojacking:** Malicious scripts embedded in websites that mine cryptocurrency when visited.
- **File-Based Cryptojacking:** Malware that infects devices to perform mining activities.
- **Mitigation:**
 - Use anti-malware solutions that detect and block cryptojacking scripts.
 - Monitor system performance for signs of unusual activity.
 - Educate users on avoiding suspicious websites and downloads.

3.5 Regulatory Bodies and Policy Frameworks

In India, regulatory bodies and policy frameworks play a pivotal role in orchestrating a robust cybersecurity landscape. Entities such as the Indian Computer Emergency Response Team (CERT-In) and the National Critical Information Infrastructure Protection Centre (NCIIPC) spearhead initiatives to safeguard the nation's cyber environment. These bodies are instrumental in developing and enforcing comprehensive policies that mandate adherence to security protocols, promote best practices, and facilitate incident response.

Policy frameworks like the National Cyber Security Policy and guidelines under the Information Technology Act provide a structured approach to cybersecurity, addressing the diverse needs of sectors ranging from finance to infrastructure. They establish clear standards for data protection, cyber resilience, and risk management, ensuring a cohesive national strategy. Furthermore, these frameworks encourage collaboration between public and private sectors, fostering

an ecosystem of shared knowledge and resources.

By continually updating regulations to keep pace with emerging threats and technological advancements, regulatory bodies and policy frameworks in India ensure a proactive stance against cyber risks, thereby fortifying the country's digital sovereignty and economic stability.

3.6 Regulatory Bodies

India's digital landscape is expanding rapidly, necessitating robust regulatory frameworks to safeguard cyberspace. Various regulatory bodies have been established to oversee cybersecurity, ensure compliance with laws, and respond to cyber threats. India's regulatory bodies play a crucial role in enhancing the country's cybersecurity posture by formulating policies, issuing guidelines, monitoring compliance, and responding to cyber threats.



The coordinated efforts of MeitY, CERT-In, NCIIPC, NCCC, RBI, and TRAI ensure a comprehensive approach to cybersecurity, addressing the unique challenges of different sectors and protecting the nation's critical information infrastructure. As cyber threats continue to evolve, these regulatory bodies remain agile and proactive in their efforts to secure India's digital landscape.

3.6.1 Ministry of Electronics and Information Technology (MeitY)

- **Role and Responsibilities:**
 - **Policy formulation:** MeitY is responsible for formulating national

policies related to information technology, including cybersecurity policies and strategies.

- **Implementation and oversight:** It oversees the implementation of cybersecurity measures and initiatives, ensuring adherence to national policies.
- **Promoting cybersecurity practices:** The ministry promotes best practices, standards, and guidelines for cybersecurity across various sectors.
- **Key Initiatives:**
 - **Digital India Program:** Aims to develop the nation towards a digitally empowered and knowledgeable economy.
 - **Cyber Surakshit Bharat Initiative:** Focuses on raising awareness and building capacities in cybersecurity.

3.7 Indian Computer Emergency Response Team (CERT-In)

3.7.1 Role and Responsibilities:

- **Incident response:** CERT-In acts as the national nodal agency for responding to cybersecurity incidents. It coordinates with various stakeholders to manage and mitigate cyber threats.
- **Threat intelligence and alerts:** It provides threat intelligence; issues alerts and advisories on cyber threats and disseminates information on vulnerabilities and best practices.
- **Capacity building:** CERT-In conducts training programs, workshops, and exercises to enhance the cybersecurity capabilities of government agencies, private sector entities, and individuals.

3.7.2 Key Initiatives:

- **Cyber Swachhta Kendra:** A Botnet Cleaning and Malware Analysis Centre

aimed at detecting and removing botnet infections.

- **Cybersecurity Drills:** Regularly conducts national and international cybersecurity drills to test and improve incident response capabilities.

3.8 National Critical Information Infrastructure Protection Centre (NCIIPC)

3.8.1 Role and Responsibilities:

- **CII protection:** NCIIPC is tasked with the protection of Critical Information Infrastructure (CII) in India, which includes sectors such as banking, finance, telecommunications, energy, and defense.
- **Risk assessment and management:** Conducts risk assessments, vulnerability analyses, and implements measures to protect CII from cyber threats.
- **Coordination and collaboration:** Collaborates with sectoral CERTs, government agencies, and private sector entities to ensure a coordinated approach to CII protection.

3.8.2 Key Initiatives:

- **Sectoral CERTs:** Establishment of sector-specific Computer Emergency Response Teams to address unique cybersecurity challenges in different CII sectors.
- **Information Sharing:** Facilitates the sharing of threat intelligence and best practices among stakeholders.

3.9 National Cyber Coordination Centre (NCCC)

3.9.1 Role and Responsibilities:

- **Real-Time monitoring:** NCCC provides real-time situational awareness of cyber threats by monitoring and analyzing cyber activities across the country.
- **Coordination and response:** Coordinates responses to cybersecurity

incidents, ensuring timely and effective action.

- **Threat analysis and intelligence:** Analyses cyber threats and disseminates intelligence to relevant stakeholders for proactive threat mitigation.

3.9.2 Key Initiatives:

- **Cyber Threat Analysis:** Conducts continuous monitoring and analysis of cyber threats to provide actionable intelligence.
- **Incident Coordination:** Facilitates coordination among various agencies and stakeholders during cyber incidents.

3.10 Reserve Bank of India (RBI)

3.10.1 Role and Responsibilities:

- **Regulation of financial sector:** RBI oversees cybersecurity in the banking and financial sector, ensuring that banks and financial institutions implement robust cybersecurity measures.
- **Guidelines and standards:** Issues guidelines and standards for cybersecurity practices in the financial sector, including requirements for risk assessment, incident response, and data protection.
- **Supervision and audits:** Conducts regular audits and inspections to ensure compliance with cybersecurity guidelines.

3.10.2 Key Initiatives:

- **Cybersecurity Framework for Banks:** Establishes a comprehensive cybersecurity framework for the banking sector, focusing on risk management, incident response, and governance.
- **Cyber Drills and Simulations:** Conducts cyber drills and simulations to test and improve the cybersecurity readiness of financial institutions.

3.11 Telecom Regulatory Authority of India (TRAI)

3.11.1 Role and Responsibilities:

- **Regulation of telecom sector:** TRAI regulates cybersecurity practices within the telecommunications sector, ensuring the security of telecom networks and services.
- **Standards and guidelines:** Develops and enforces standards and guidelines for securing telecom infrastructure and protecting consumer data.
- **Monitoring and compliance:** Monitors compliance with cybersecurity regulations and takes corrective actions as necessary.



3.11.2 Key Initiatives:

- **Telecom Security Guidelines:** Issuance of guidelines for the security of telecom networks and services.
- **Consumer Awareness:** Promotes awareness among consumers about cybersecurity risks and best practices.

3.12 Policy Frameworks

India has made substantial progress in developing its cybersecurity framework. Key initiatives include the establishment of the Indian Computer Emergency Response Team (CERT-In), the National Cyber Security Policy 2013, and various sector-specific guidelines as follows:

- National Cybersecurity Strategy, 2020
- National Cybersecurity Policy, 2013
- Information Technology Act, 2000

Despite these efforts, the country continues to face numerous cybersecurity challenges.



3.13 National Cybersecurity Policy, 2013

The National Cybersecurity Policy of 2013 is a comprehensive framework established by the Government of India aimed at protecting the country's information infrastructure and managing the associated risks. This policy was introduced in response to the increasing threat landscape and the need for a robust cybersecurity strategy to safeguard critical information infrastructure.

3.13.1 Objectives of the Policy:

- **To create a secure Cyber Ecosystem:** The policy emphasizes the creation of a secure and resilient cyber ecosystem within the country. This involves establishing necessary regulatory frameworks, enabling legal, technical, and operational measures to address cyber threats.
- **Enhancing capacities:** A key goal is to enhance the capabilities of various stakeholders including government entities, businesses, and individuals to effectively respond to and mitigate cyber threats. This includes training and awareness programs aimed at improving the cybersecurity posture.
- **Strengthening regulatory frameworks:** The policy aims to strengthen existing legal frameworks to address the issues of cybercrime more effectively. This includes updating laws, improving enforcement mechanisms, and ensuring international cooperation.
- **Promoting research and development:** Encouraging R&D in cybersecurity technologies is a significant component of the policy. This involves supporting innovation and the development of new technologies to counter evolving cyber threats.
- **Protection of Critical Information Infrastructure (CII):** The policy prioritizes the protection of CIIs such as banking, telecommunications, defence, energy, and other vital sectors. It aims to develop a robust framework for identifying, assessing, and mitigating risks to these infrastructures.

3.13.2 Key Components:

- **Institutional Structures:** The policy calls for the establishment of various bodies and institutions to oversee and implement cybersecurity measures. This includes the National Critical Information Infrastructure Protection Centre (NCIIPC) responsible for securing critical information infrastructure.
- **Cybersecurity Assurance Framework:** It includes the development of frameworks to ensure that all entities handling critical data comply with prescribed cybersecurity standards and best practices.
- **Public–Private Partnerships:** Recognizing the role of private sector entities in managing and operating critical infrastructure, the policy promotes collaboration between public and private sectors for effective cybersecurity management.
- **Information Sharing and Cooperation:** The policy encourages the creation of mechanisms for sharing threat intelligence and information on vulnerabilities among various stakeholders, both nationally and internationally.
- **Capacity Building and Skill Development:** It stresses the need for enhancing the skills of professionals working in the field of cybersecurity through specialized training programs and certifications.

3.13.3 Challenges and Implementation:

While the National Cybersecurity Policy, 2013, sets a robust foundation for securing India's cyberspace, its implementation has faced several challenges.

These include:

- **Coordination among stakeholders:** Ensuring effective coordination among various government agencies, private sector entities, and international partners remains a complex task.
- **Resource constraints:** Allocating sufficient resources, both financial and human, to implement various measures outlined in the policy has been

challenging.

- **Rapid technological advancements:** Keeping up with the fast-paced evolution of cyber threats and technologies requires continuous updates to the policy and associated frameworks.
- **Awareness and training:** Ensuring widespread awareness and training across all levels of society, from government officials to the general public, is an ongoing effort.

The National Cybersecurity Policy, 2013, marks a significant step towards building a secure and resilient cyberspace in India. It lays down a comprehensive strategy for addressing the multifaceted challenges of cybersecurity. While the policy provides a strong foundation, continuous efforts in terms of coordination, resource allocation, and adaptation to emerging threats are essential for its successful implementation and for safeguarding India's critical information infrastructure.

3.14 Information Technology Act, 2000

The Information Technology Act, 2000, is a landmark legislation in India that provides a legal framework for electronic governance and addresses issues related to cybercrime and electronic commerce. Enacted on October 17, 2000, this act represents a crucial step towards adapting the country's legal framework to the digital age, ensuring that electronic transactions are legally recognized and protected.

3.14.1 Objectives of the IT Act:

- **Legal recognition of electronic transactions:** One of the primary objectives of the IT Act, 2000, is to provide legal recognition to electronic records and digital signatures, thereby facilitating electronic commerce and transactions.
- **Prevention of cybercrime:** The Act addresses various types of cybercrimes, including hacking, identity theft, and digital fraud, laying down penalties and punishments for offenders.

- **Promoting E-Governance:** The IT Act promotes the use of electronic records and digital signatures in government operations and services, enhancing efficiency and transparency.
- **Facilitating E-Commerce:** By recognizing electronic contracts and transactions, the Act aims to boost the growth of e-commerce, providing a secure and reliable environment for digital business activities.

3.14.2 Key Provisions of the IT Act:

- **Legal recognition of electronic records:** Sections 4 and 5 of the Act grant legal recognition to electronic records and digital signatures, enabling their use in legal contracts, agreements, and other formal documents.
- **Digital signatures:** The Act defines digital signatures and outlines the process for their authentication, making them equivalent to handwritten signatures in electronic transactions.
- **Regulation of Certifying Authorities:** The Act establishes a framework for the regulation of certifying authorities, which are responsible for issuing digital certificates and ensuring the security of digital signatures.
- **Cybercrimes and penalties:** Chapter XI of the Act specifies various cybercrimes and prescribes penalties and punishments for offences such as hacking, unauthorized access, identity theft, and cyber terrorism.
- **Adjudication of disputes:** The Act provides for the appointment of adjudicating officers to handle disputes related to electronic transactions and cybercrimes, ensuring a streamlined process for resolution.
- **Establishment of the Cyber Appellate Tribunal:** The Act establishes the Cyber Appellate Tribunal to hear appeals against the orders of adjudicating officers, providing a higher level of judicial oversight.
- **Offences by Intermediaries:** The Act outlines the liability of intermediaries, such as internet service providers and web hosting services, for third-party content. It provides them with a safe harbour if they follow due diligence and

take necessary actions upon receiving complaints.

3.14.3 Amendments and updates:

The IT Act, 2000, has undergone several amendments to address the evolving nature of cyber threats and technological advancements. The most significant amendment came in 2008, which introduced several new provisions, including:

- **Cyber Terrorism:** The act now includes provisions to address cyber terrorism, defining it and prescribing severe penalties for those involved in cyber terrorism activities.
- **Obscenity and Pornography:** The amendment expanded the scope of the Act to include offences related to the publication and transmission of obscene material, including child pornography.

3.14.4 Challenges:

Despite its comprehensive nature, the IT Act, 2000, has faced several challenges and criticisms:

- **Ambiguity and interpretation:** Some provisions of the Act have been criticized for being vague and open to interpretation, leading to potential misuse and arbitrary enforcement.
- **Implementation and enforcement:** Effective implementation and enforcement of the Act's provisions remain a challenge due to a lack of awareness, inadequate resources, and technical expertise among law enforcement agencies.

The Information Technology Act, 2000, serves as a foundational legal framework for governing electronic transactions and combating cybercrime in India. It has played a pivotal role in fostering the growth of e-commerce, promoting e-governance, and enhancing cybersecurity. However, continuous efforts to update and refine the Act are essential to address emerging cyber threats and technological advancements, ensuring that it remains relevant and effective in the digital age.

3.15 National Cybersecurity Strategy, 2020

The National Cybersecurity Strategy, 2020, represents a significant step forward in India's efforts to secure its cyberspace against evolving threats. This strategy, developed by the National Security Council Secretariat (NSCS), aims to create a safe, secure, and resilient cyberspace for citizens, businesses, and the government.

3.15.1 Objectives of the Strategy:

- **Secure National Cyberspace:** The primary goal is to secure India's cyberspace from cyber threats by enhancing the protection of critical information infrastructure and creating a robust cybersecurity framework.
- **Strengthen institutions and capacities:** The strategy aims to build and strengthen institutions and capacities across sectors to respond effectively to cybersecurity incidents.
- **Promote cyber awareness and skills:** Enhancing cyber awareness among citizens and promoting the development of skills and competencies in cybersecurity is a key focus.
- **Foster international cooperation:** The strategy emphasizes the importance of international cooperation in tackling cyber threats and establishing norms for responsible state behaviour in cyberspace.

3.15.2 Key Pillars of the Strategy:

- **Critical Information Infrastructure (CII) protection:** The strategy outlines measures to identify and protect CII sectors such as banking, telecommunications, energy, and defence. This includes regular risk assessments, vulnerability management, and the establishment of robust incident response mechanisms.
- **Institutional framework and governance:** Strengthening the existing institutional framework, including the role of agencies like the Indian Computer Emergency Response Team (CERT-In) and the National

Critical Information Infrastructure Protection Centre (NCIIPC), to ensure a coordinated response to cyber incidents.

- **Capacity building and skill development:** Developing a skilled cybersecurity workforce through education, training, and certification programs. This includes integrating cybersecurity education into school and university curricula and promoting research and development in cybersecurity technologies.
- **Cybercrime prevention and law enforcement:** Enhancing the capabilities of law enforcement agencies to prevent, detect, investigate, and prosecute cybercrimes. This involves updating legal frameworks, improving digital forensics capabilities, and fostering cooperation with international law enforcement agencies.
- **Public–Private partnership:** Encouraging collaboration between government and private sector entities to share information on threats and vulnerabilities and to develop joint strategies for protecting cyberspace.
- **Cyber hygiene and awareness:** Promoting cyber hygiene practices among individuals and organizations to prevent cyber incidents. This includes public awareness campaigns, workshops, and the dissemination of best practices for cybersecurity.
- **International engagement:** Engaging with international partners to share best practices, participate in global cybersecurity initiatives, and contribute to the development of international norms and standards for cybersecurity.

3.16 Strategic Actions and Initiatives

- **National Cybersecurity Coordination Centre (NCCC):** Operationalizing the NCCC to provide real-time situational awareness and coordinate responses to cybersecurity incidents.
- **Cybersecurity training and certification:** Establishing national-level programs for cybersecurity training and certification to ensure a steady pipeline of skilled professionals.

- **Sectoral CERTs:** Creating sector-specific Computer Emergency Response Teams (CERTs) to address unique cybersecurity challenges in different sectors.
- **Research and innovation:** Promoting research and innovation in cybersecurity through funding, grants, and partnerships with academic institutions and industry.
- **Legislative measures:** Reviewing and updating existing cybersecurity laws and regulations to address emerging threats and challenges. This includes developing a robust data protection framework.
- **Challenges and Implementation:** The implementation of the National Cybersecurity Strategy, 2020, faces several challenges:
 - **Coordination and collaboration:** Ensuring effective coordination among various stakeholders, including government agencies, private sector entities, and international partners.
 - **Resource allocation:** Allocating adequate resources, both financial and human, to implement the strategy's initiatives effectively.
 - **Rapid technological changes:** Keeping pace with the fast-evolving cyber threat landscape and technological advancements.
 - **Awareness and education:** Promoting widespread awareness and understanding of cybersecurity among the general public and organizations.

The National Cybersecurity Strategy, 2020, is a comprehensive framework aimed at securing India's digital infrastructure and ensuring a resilient cyberspace. By focusing on critical information infrastructure protection, capacity building, public-private partnerships, and international cooperation, the strategy aims to create a robust cybersecurity ecosystem. Successful implementation of this strategy is essential to protect national interests, promote economic growth, and safeguard the digital lives of Indian citizens in an increasingly interconnected world.

3.17 Challenges in Cybersecurity

While there are multiple cybersecurity policies and guidelines, their implementation and enforcement are inconsistent across sectors. The pace of technological change outstrips the development of corresponding security measures, creating vulnerabilities that can be exploited by cybercriminals. A significant portion of the population remains unaware of basic cybersecurity practices. This lack of awareness extends to small and medium enterprises (SMEs), making them easy targets for cyberattacks. **Major challenges include:**

- **Sophistication of cyber attacks by using new methods and tools**
- **Rapid technological advancements**
- **Evolving regulatory and compliance issues**
- **Shortage of skilled cybersecurity defenses**
- **Inadequate cybersecurity awareness**
- **Emergence of cybersecurity attacks beyond geographical boundaries**

3.18 Enhancing Cybersecurity Posture

Cybersecurity posture refers to the overall strength and readiness of an organization or a nation to protect its information assets and respond to cyber threats. It encompasses the policies, procedures, technologies, and human resources dedicated to securing digital infrastructure. As India rapidly embraces digital transformation across various sectors, enhancing cybersecurity posture has become a national imperative. The country's growing digital footprint, driven by initiatives like Digital India, e-Governance, and increased internet penetration, necessitates a robust and dynamic approach to cybersecurity.

Key strategies for enhancing cybersecurity posture in India:

3.18.1 Strengthening Regulatory Frameworks:

- **Data Protection legislation:** Enactment of comprehensive data protection

laws to safeguard personal and sensitive data. While the Digital Personal Data Protection Act has been formulated, specifying rules to ensure proper implementation is in progress.

- **Regular audits and compliance:** Mandatory cybersecurity audits and compliance checks for critical sectors to ensure adherence to established security protocols.

3.18.2 Capacity Building and Skill Development:

- **Cybersecurity education:** Incorporating cybersecurity education into school and university curricula to build a future-ready workforce. Specialized courses and certifications for professionals to enhance their skills.
- **Training programs:** Conducting regular training programs for government officials, law enforcement, and private sector employees to stay updated on the latest cybersecurity practices and technologies.

3.18.3 Public-Private Partnerships:

- **Collaborative frameworks:** Establishing collaborative frameworks for information sharing and joint initiatives between the government and private sector. This includes threat intelligence sharing, joint incident response exercises, and collaborative research projects.
- **Industry engagement:** Encouraging industry associations to develop sector-specific cybersecurity guidelines and best practices.

3.18.4 Technological Advancements:

- **Advanced security technologies:** Adoption of advanced technologies such as artificial intelligence, machine learning, and blockchain to enhance threat detection, incident response, and data integrity.
- **Secure infrastructure:** Investment in secure and resilient infrastructure, including secure data centres, encrypted communication channels, and robust network security measures.

3.18.5 Critical Information Infrastructure (CII) Protection:

- **Risk assessment and management:** Regular risk assessments and vulnerability analyses of critical information infrastructure to identify and mitigate potential threats.
- **Sectoral CERTs:** Establishment of sector-specific Computer Emergency Response Teams (CERTs) to address unique cybersecurity challenges in critical sectors like finance, healthcare, energy, and defense.

3.18.6 Cyber Hygiene and Awareness:

- **Public awareness campaigns:** Nationwide campaigns to promote cyber hygiene practices among citizens, businesses, and government employees. This includes awareness on phishing, secure password practices, and recognizing cyber threats.
- **Best practices dissemination:** Development and dissemination of cybersecurity best practices guides and toolkits for various stakeholders.

3.18.7 Incident Response and Recovery:

- **Incident response teams:** Formation of dedicated incident response teams at national and organizational levels to handle cybersecurity incidents promptly and effectively.
- **Recovery plans:** Development of comprehensive incident response and disaster recovery plans to ensure quick recovery from cyber incidents and minimize impact.

3.18.8 International Cooperation:

- **Global partnerships:** Active participation in global cybersecurity initiatives and collaborations with international organizations and countries to share best practices and tackle cross-border cyber threats.
- **Norms and standards:** Contributing to the development of international norms and standards for responsible state behaviour in cyberspace.

3.18.9 Challenges and Opportunities:

- **Challenges:**
 - **Resource constraints:** Limited financial and human resources dedicated to cybersecurity can hinder the implementation of robust security measures.
 - **Evolving threat landscape:** Rapidly changing cyber threats require continuous adaptation and updating of security strategies and technologies.
 - **Awareness gap:** A significant gap in cybersecurity awareness among the general public and small businesses, making them vulnerable to cyber-attacks.

- **Opportunities:**
 - **Technological innovations:** Leveraging emerging technologies to enhance cybersecurity measures and develop innovative solutions to tackle cyber threats.
 - **Government initiatives:** Leveraging government initiatives like Digital India and Startup India to promote cybersecurity startups and innovation.
 - **Global leadership:** Establishing India as a global leader in cybersecurity through active participation in international forums and setting high standards for cybersecurity practices.

3.19 Conclusion

Enhancing India's cybersecurity posture is crucial for safeguarding its digital economy, protecting critical infrastructure, and ensuring the security of its citizens in an increasingly digital world. By strengthening regulatory frameworks, building capacity, fostering public-private partnerships, embracing technological advancements, and promoting cyber awareness, one can create a robust and

resilient cybersecurity ecosystem. Addressing the challenges and leveraging opportunities will be key to achieving this goal.

3.19.1 Responsibility to Manage Cybersecurity

- Managing cybersecurity in an organization is a multifaceted responsibility that involves various roles, departments, and stakeholders working together to protect the organization's digital assets and data. While the ultimate accountability for cybersecurity often lies with top leadership, several key roles and functions are crucial to maintaining a robust cybersecurity posture.
- In today's interconnected world, cybersecurity is not solely the responsibility of the IT or security departments; it's a collective effort that involves every individual within an organization. Effective cybersecurity management is a shared responsibility across all levels of an organization. Executives provide the leadership and resources, IT and security teams implement and monitor defenses, managers enforce policies, and employees adhere to best practices and report issues. By working together, everyone can contribute to a robust security posture, protecting the organization from the ever-evolving landscape of cyber threats.

4.1 Standards on Internal Audit (Global and ICAI Pronouncements)

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.

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.

- **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.

4.2 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:

4.2.1 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.

4.2.2 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.

4.2.3 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:** Offer specific requirements for assurance and consulting services.

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

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

4.3 ICAI's Standards on Internal Audit (SIAs)

The Institute of Chartered Accountants of India (ICAI) has played a leading role in this process by developing a comprehensive framework for the internal audit function and education to internal auditors. The ICAI has also established a certification program for internal auditors, which is recognized by the government.



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 the 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.

4.3.1 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.

4.3.2 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

Series	Standard No	Title
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

4.3.3 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.

- o Promotes alignment with organizational goals and priorities.

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

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

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

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

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

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

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

- o Highlights the importance of effective communication with governance bodies.
- o Recommends periodic updates on audit progress and

significant findings.

- o 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**

- o Provides a structured approach to planning individual audit assignments.
- o Emphasizes understanding the audit area and setting clear objectives.
- o Stresses resource allocation and time management.

- **SIA 320: Internal Audit Evidence**

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

- **SIA 330: Internal Audit Documentation**

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

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

- o Emphasizes the need for supervision during audit

assignments.

- o Recommends periodic reviews to ensure adherence to audit standards.
- o Focuses on quality control and professional development.

➤ **SIA 360: Communication with Management**

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

➤ **SIA 370: Reporting Results**

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

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

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

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

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

- o Focuses on auditing IT systems, controls, and cybersecurity measures.
- o Highlights the importance of data integrity, privacy, and system reliability.
- o Recommends staying updated on evolving technology risks.
- **SIA 530: Third Party Service Provider**
 - o Guides auditors on assessing risks associated with outsourcing.
 - o Emphasizes evaluating third-party compliance and performance.
 - o Focuses on ensuring contract terms align with organizational goals.
- **Standards Issued up to July 1, 2013**
 - **SIA 5: Sampling**
 - o Explains methodologies for selecting representative samples.
 - o Emphasizes accuracy and reliability in sample-based audits.
 - o Recommends statistical and non-statistical sampling techniques.
 - **SIA 6: Analytical Procedures**
 - o Guides auditors on using analytics to identify trends and anomalies.
 - o Recommends integrating data analysis in risk-based audits.
 - o Focuses on cost-effective and efficient audit practices.
 - **SIA 7: Quality Assurance in Internal Audit**

- o Highlights the importance of quality parameters in audits.
 - o Recommends periodic reviews and adherence to professional standards.
 - o Encourages continuous improvement through feedback and training.
- **SIA 11: Consideration of Fraud in an Internal Audit**
- o Provides a framework for identifying potential fraud risks.
 - o Recommends proactive measures to detect and mitigate fraud.
 - o Focuses on ensuring ethical practices within the organization.
- **SIA 18: Related Parties**
- o Guides auditors on identifying and auditing related-party transactions.
 - o Emphasizes transparency and compliance with disclosure requirements.
 - o Recommends ensuring fairness and preventing conflicts of interest.

5.1 Banking Sector

5.1.1 Regulatory Framework

Banking companies operate within a defined statutory framework that safeguard depositor's interests, enforces disclosure discipline and enable the development of the financial sector. **These acts are:**

- **Umbrella Acts**

- **Reserve Bank of India Act, 1934:** Governs the Reserve Bank's functions
- **Banking Regulation Act, 1949:** Governs the financial sector

In addition to the above, the banking operations are also subject to legal provisions contained in the certain other Acts as follows:

- **Acts governing specific functions**

- **Government Securities Act 2006:** Governs the government debt market
- **Securities Contract (Regulation) Act, 1956:** Regulates the government securities market
- **Securities and Exchange Board of India Act, 1992**
- **Coinage Act, 2011:** Governs currency and coins
- **Foreign Exchange Management Act, 1999:** Governs the trade and foreign exchange market
- **Payment and Settlement Systems Act, 2007:** Provides for regulation and supervision of payment systems in India

- **Acts governing Banking Operations**

- **Companies Act, 2013:** Governs banks as companies

- **Banking Companies (Acquisition and Transfer of Undertakings) Act, 1970 / 1980:** Relates to nationalization of banks
- **Bankers' Books Evidence Act**
- **Negotiable Instruments Act, 1881**
- **Acts governing Individual Institutions**
 - State Bank of India Act, 1955
 - The Industrial Development Bank (Transfer of Undertaking and Repeal) Act, 2003
 - The Industrial Finance Corporation (Transfer of Undertaking and Repeal) Act, 1993
 - National Bank for Agriculture and Rural Development Act
 - National Housing Bank Act
 - Deposit Insurance and Credit Guarantee Corporation Act
 - Co-operative Societies Act, 1912
 - Regional rural Banks Act, 1976
 - The State Banks (Repeal and Amendment) Act, 2018
 - Prevention of Money Laundering Act, 2002
 - Credit Information Companies Regulation Act, 2005
 - Information Technology Act, 2000
 - Securitization and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002

5.1.2 Risk Based Internal Audit (RBIA)

Banks and NBFCs need to adopt a Risk Based Internal Audit (RBIA) approach for

carrying our internal audit function. The primary focus of RBIA shall be to provide reasonable assurance to the Board and senior management about the adequacy and effectiveness of the risk management and control framework in the company's operations.

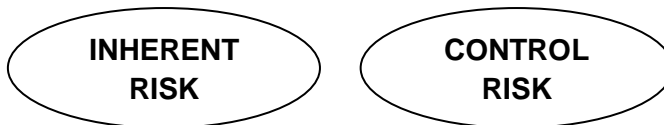
- The RBIA should focus on risk identification, deciding on priority of audit areas, and allocation of audit resources in accordance with the risk assessment. The Company's policy shall include the risk assessment methodology for identifying the risk areas based on which the audit plan would be formulated.
- **The risk assessment methodology should, inter alia, cover the following parameters:**
 - Previous internal audit reports and compliance
 - Proposed changes in business lines or change in focus
 - Significant change in management / key personnel
 - Results of latest regulatory examination report
 - Reports of external auditors
 - Industry trends and other environmental factors
 - Time elapsed since last audit
 - Volume of business and complexity of activities
 - Substantial performance variations from the budget



- **Automation and Analytical Tools Used by Banks / NBFCs**

Fincle – Universal Banking Solution	Cracle FLEXCUBE – Core Banking	TCS BaNCS – Core Banking System	Temenos – Core banking, digital banking platforms
Pennant – Loan Management System	Loan IQ – Loan Management Platform	Indus Retail Loan Management System	Omnicore – Loan Processing documents, KYC/AML, Trade Finance documents
Imex – Trade Finance Processing	Finastras – FBTI – Trade Finance Operations	SAP Concur – Travel, expense and invoice management application	AXIOM – Regulator Reporting

5.1.3 Risks in banking are classified as follows:



Inherent risks are of three types: **CREDIT RISK, MARKET RISK & OPERATIONAL RISK**

- **Credit risks** are associated with losses due to erosion in the credit quality.
Examples:
 - Interest or principle not paid by the borrower (Direct lending)
 - Funds not paid on crystallization of liability (Guarantee or Letter of Credit)
 - Free forex funds restricted (cross border exposure)
- **Market risks** relate to losses caused by changes in the market variables.

Examples:

- Inability to meet liabilities (liquidity risk)
- Adverse changes in interest rates (Interest rates risk)
- Adverse forex rates (Forex risk)
- **Operational risks** relate to losses resulting from inadequate or failed processes, people or external events. Examples:
 - People turnover, skill competency (People risk)
 - Violation of limits, money laundering (Process risk)
 - System failure, communication failure (System risk)
 - Non-compliance to laws (Legal & regulatory risk)
 - Loss of reputation (Reputation risk)
 - Unanticipated Changes (Event risk)

5.1.4 Important Areas covered in Banking and key review points

Sr. No.	Areas	Key Review Points
1	Deposit-CASA	<ul style="list-style-type: none"> ● Customer Onboarding controls, KYC, CKYC, Risk Categorization. ● Customer Due Diligence and AML Monitoring. ● Compliance with Minimum balance, interest, penalty, service charges calculation and recovery. ● Issuance of Cheque book, Debit/Credit Card, PIN. ● Monitoring of the Savings account used for commercial/business transactions instead of the Current Account. ● Review of accounts opened with deferred KYC, freeze, lien marked accounts. ● Backdated Transaction scrutiny.

Sr. No.	Areas	Key Review Points
2	Deposit-Term Deposits	<ul style="list-style-type: none"> ● End-to-end controls of Term Deposit Creation, Rate applied and any manual entries posted after proper approvals. ● Auto-Renewal, Premature Closure, Interest/penalty computation and timely credit to customer account. ● Lien Marking and reversal, monitoring of High Value TDs. ● Backdated TD booking, Manual intervention in the rate of Interest/charges. ● TDS deduction, Form 15G/H compliance and timely review of unclaimed or overdue deposits including transfer to DEAF
3	Deposits- NRO/ NRE/FCNR	<ul style="list-style-type: none"> ● Customer Classification, Residential status and FEMA compliance. ● Inward remittances, repatriation limits, and misuse of domestic routing. ● Currency management and exchange rate application. ● TDS applicability, DTAA and Form 15CA/CB compliance. ● Residential status change and validation of Power of Attorney (POA) transactions.
4	KYC/AML	<ul style="list-style-type: none"> ● Compliance with RBI KYC Master Direction and AML Regulations, RBI Video KYC guidelines and prescribed onboarding procedure. ● KYC onboarding and Customer Due Diligence process. ● Enhanced Due diligence for High Risk and PEP customers. ● Customer Risk Categorisation and Re-KYC process. ● Name Screening and Watchlist Monitoring. ● PAN / Aadhar Validation and De-Dupe Controls.

Sr. No.	Areas	Key Review Points
		<ul style="list-style-type: none"> ● Handling of Customers with multiple CIFs. ● Authenticity of customer identity verification, document validation and UIDAI/NSDL checks. ● Effectiveness of live verification controls, liveness detection and geo tagging. ● Retention of Physical and Video KYC records, audit trails and data security.
5	Corporate Advances- Term Loans	<ul style="list-style-type: none"> ● Financial Viability, Credit Rating, Due diligence. ● Stage wise disbursement and end-use verification. ● Monitoring of EMI Repayment, Moratorium adherence, early warning stress signal.
6	Corporate Advances- Project Financing	<ul style="list-style-type: none"> ● Project appraisal via Detailed Project Report (DPR). ● Verification of Property Title, Regulatory clearances and pre-disbursement conditions. ● Project insurance adequacy and validity till completion of project cycle. ● Equity Claw back Risk. ● Drawdown amount not used for a prolonged period.
7	SWIFT Reconciliation	<ul style="list-style-type: none"> ● Completeness and accuracy of SWIFT message and proper mapping to GL and Nostro entries. ● Timely reconciliation of SWIFT transactions and resolution for unmatched, failed, duplicate and pending messages. ● Control on SWIFT message authenticity, authorization, format accuracy, overrides and manual intervention. ● Effectiveness of system and user access controls, audit logs and operational continuity during downtime. ● Accuracy of SWIFT-related charges and recoveries.
8	Internal Office Accounts	<ul style="list-style-type: none"> ● Control and monitoring of internal account lifecycle (opening, operation, closure)

Sr. No.	Areas	Key Review Points
		<ul style="list-style-type: none"> ● Completeness of GL postings and reversals. ● Controls for NPA concealment, fund diversion and manipulation. ● Monitoring settlements, provisioning, write-off. ● Adherence to regulatory norms, exceptions and transaction monitoring.
9	Retail Advances- Mortgages	<ul style="list-style-type: none"> ● Property Title, Mortgage Creation (CERSAI) and Legal Due diligence. ● Independent Property Valuation, Technical Inspection and LTV Compliance. ● Controls on Disbursement and End Use for Under construction property. ● Completeness of Loan agreement and secured custody of the mortgaged property document, Original Title Deed etc. ● Monitoring of Repayment and adherence of recovery under the SARFAESI Act.
10	Retail Advances- Vehicle Finance	<ul style="list-style-type: none"> ● End-to-end process of borrower eligibility, credit bureau rating, dealer empanelment and validation of vehicle. ● Disbursement controls, physical verification of the vehicle and hypothecation marking with RTO ● Insurance Coverage adequacy. ● Monitoring of EMI Repayment, Penalty and Charges. ● Controls on repossession and recovery in case of default
11	Retail Advances- Gold Loans	<ul style="list-style-type: none"> ● Gold Appraisal and Purity Testing. ● Process of Pledge Creation, Photographic evidence and Tamper-proof packet sealing. ● Dual Vault Custody, CCTV Monitoring, Monitoring of Gold Packet movements and Insurance adequacy. ● Governance over auction and recovery.

Sr. No.	Areas	Key Review Points
		<ul style="list-style-type: none"> ● Unreleased gold post loan closure.
12	Retail Advances- Personal Loans	<ul style="list-style-type: none"> ● Customer Eligibility and KYC Verification. ● Income Proof Validation. ● Completeness of the Loan agreement, Sanction Terms and Conditions, NACH Mandate and borrower's acknowledgment. ● Control on the disbursement of amounts and EMI Repayment monitoring. ● Adherence to Fair recovery and collection practices.
13	Credit Cards	<ul style="list-style-type: none"> ● Credit limit assignment based on credit bureau score and income/KYC verification. ● Card activation, PIN generation and transaction authentication controls. ● Pre-approved and instant credit card issuance controls. ● Enable/Disable of E-commerce, domestic and international card usage and limit. ● Billing Cycle, Minimum due, interest and penalty calculation.
14	Retail Advances- Priority Sector Lending	<ul style="list-style-type: none"> ● Priority Sector Lending (PSL) Classification (Agriculture, MSME etc), Borrower eligibility and compliance with regulatory norms. ● Segment specific controls, MSME Registration, Udhyan Verification and End Use Validation. ● Correctness and Completeness of PSL Returns filed with RBI. ● Portfolio Concentration Risk. ● Compliance with Interest Subvention for the specific PSL Scheme.
15	Clearing and Settlements	<ul style="list-style-type: none"> ● End-to-end settlement verification of source system, GL and settlement files. ● Unreconciled entries posted in suspense account

Sr. No.	Areas	Key Review Points
		<p>ageing, root cause and clearance.</p> <ul style="list-style-type: none"> ● Monitoring of Real time settlement, authorization, reversal and failed transactions for RTGS/NEFT. ● Controls on the Cheque Truncation process, image quality standard, fraud detection and return handling.
16	Branch Banking Operations	<ul style="list-style-type: none"> ● Adherence to customer transactions and service requests. ● Control over cash handling, vault operations and daily balancing. ● Maintenance of records, registers and operational discipline. ● Overall effectiveness of physical security, restricted area access controls. ● Effectiveness of customer service including complaint resolution, service quality and TAT.
17	Inoperative Accounts/DEAF	<ul style="list-style-type: none"> ● Identification and monitoring of transactions in Inoperative account. ● Controls on Reactivation post KYC and CDD compliance. ● Verification of Interest Credited and Service Charges applied in an inoperative account. No penalty to be collected for non-usage of account. ● Correctness and completeness of balances transferred in DEAF after 10 years of inactivity. ● Adherence to DEAF Claim Settlement procedure, customer grievance handling and Regulatory reporting to RBI.
18	Outsourced Vendors	<ul style="list-style-type: none"> ● Compliance with RBI guidelines on outsourcing of services. ● Vendor Onboarding and due diligence process. ● Review of Service level agreement (SLA), data confidentiality, security and data sharing controls clause, exit clause.

Sr. No.	Areas	Key Review Points
		<ul style="list-style-type: none"> ● Review Vendor business continuity plan. ● Monitoring of vendor activity and performance in compliance with SLA. ● Rotation of vendor. ● Control over billing verification and payment processing.
19	Central Processing Centres / Regional Processing Centres	<ul style="list-style-type: none"> ● Adherence to Centralized Standard Operation Procedure (SOP) and control framework. ● Assess Maker-Check control and Segregation of Duty. ● Data entry correctness and completeness vis-à-vis documents. ● Turnaround Time (TAT) adherence, backlog management and monitoring of ageing cases. ● Control the exception, rejection and escalation process. ● Control the re-opening of already processed cases. ● Verification of manual override data entries during system downtime. ● Validation of auto decision BOTs. ● User rights access provided/modified with approvals. ● System access controls and audit trail.
20	Government Business Module (PF/SSY/PMKVPY/ Pension)	<ul style="list-style-type: none"> ● Compliance to scheme-specific regulatory guidelines issued by the government. ● Customer Eligibility for onboarding and KYC compliance. ● Verification of contribution limits, maximum deposit cap, tenure and scheme specific terms and conditions. ● Controls on claim processing and premature closure. ● Assess the process for the detection of duplicate accounts for the same scheme.

Sr. No.	Areas	Key Review Points
		<ul style="list-style-type: none"> ● Monitoring of Inactive accounts and unclaimed balances. ● Validation of data submission and reporting to government authorities.
21	Remittances	<ul style="list-style-type: none"> ● Controls on Inward/Outward Remittances and FEMA Compliance. ● Foreign Remittance Purpose Code Validation. ● Remitter and Beneficiary KYC and CDD compliance. ● SWIFT Message Reconciliation vis-à-vis inward/outward remittance. ● Review of Exchange Rate and charges applied.
22	Currency Chest Management	<ul style="list-style-type: none"> ● Adherence to RBI guidelines on Currency Chest operations. ● Reconciliation of Physical Cash and System balances. ● Strong room access controls and surveillance. ● Counterfeit Note detection, impounding and reporting process. ● Soiled and mutilated notes segregation, storage and remittance. ● Daily position reporting and remittances to RBI. ● Verify the process of cash movement between branches, the Chest and RBI. ● ATM Cash Loading/Unloading and reconciliation with the chest balance.
23	Digital/Mobile Banking	<ul style="list-style-type: none"> ● Compliance with RBI Digital Banking and Cyber Security guidelines. ● User authentication controls, access and session time out management. ● Data Security and Encryption controls. ● Application security, vulnerability assessment and patch management. ● Application programming interface (API) Security

Sr. No.	Areas	Key Review Points
		<p>and Third-Party integration controls.</p> <ul style="list-style-type: none"> ● Digital Onboarding of customers and E-KYC/V-KYC controls. ● Geo Location and IP-based monitoring controls. ● Deactivation, reactivation of digital user IDs. ● Controls over Transaction limit, failed transaction and reversal controls. ● Customer awareness and communication on digital fraud risk.
24	Record Management Unit	<ul style="list-style-type: none"> ● Compliance with applicable regulatory and statutory record retention guidelines. ● Alignment of the approved record retention matrix vs. the actual matrix. ● Review custody and security of Physical Records, strong room access controls and surveillance. ● Controls for maintaining the authenticity and integrity of scanned documents. ● Compliance with Data Protection Law. ● Business Continuity and Disaster Recovery Plan adequacy. ● Destruction of Records and documents with approvals and logs. ● Review of Indexing, Barcode Tagging, scanning quality and completeness of documents. ● Periodic Stock Verification, Document movement tracking and Reconciliation of Physical and Digital Records. ● Assessment of Storage Space usage in alignment with the agreed space capacity.
25	International Business Unit- GIFT CITY (IBU/	<ul style="list-style-type: none"> ● Compliance with IFSCA, RBI and FEMA guidelines applicable to GIFT City. ● Offshore and NRI customer onboarding, KYC/AML

Sr. No.	Areas	Key Review Points
	GIFT City)	<p>and EDD compliance.</p> <ul style="list-style-type: none"> ● Foreign Currency Transaction Monitoring, settlement and reconciliation. ● SWIFT message controls for cross-border settlements. ● Trade Finance transaction compliance.

5.2 Insurance Sector

5.2.1 Regulatory Framework Governing the Insurance Sector

- **Insurance Act, 1938** – It is the principal Act governing the Insurance Business in India.
- **IRDA Act, 1999** – This Act deals with the formation of IRDA as a Controlling Body of Insurance in India. The Act states the regulatory provisions regarding the rights and functioning of IRDA.
- **LIC Act, 1956** – Provides for the constitutional framework for the functioning of LIC of India
- **GIC Act, 1972** – Provides for the constitutional framework for the functioning of GIC of India
- **Companies Act, 2013** – All the new Insurance companies being Body Corporate are governed by the provisions of this Act.
- **Insurance Council** – Insurance Councils are formed for Life and Non-life Insurance with all the CEO of Insurance companies as their members. Two members are nominated by IRDA, one of whom is chairperson of the council. Important matters related to the Insurance Business are discussed in the Insurance Councils.



- **Insurance Ombudsman** – Insurance Councils appoint an Insurance Ombudsman to deal with Policyholders' complaints related to claims, premiums and policy servicing. They can deal with matters where dispute up to Rs. Twenty lacs is involved. Their report is binding on the insurer, but not on the policyholder. At present, there are twelve Ombudsmen functioning all over India.

5.2.2 Major Sub Segments of the Insurance Sector

- **Life Insurance**– Human life has economic value as the sudden loss of life of a breadwinner can create tremendous hardship for his family. Life Insurance provides for the lump sum required by the family to maintain its standard of living in case of the unfortunate death of the breadwinner.

Similarly, life insurance is used as a hedge against the possible loss incurred due to the death of a person through the following arrangements–

- a) Key Man Insurance
- b) Partnership Insurance
- c) Employer Employee Scheme
- d) Debtors' Insurance

Insurance policies with a provision of a lump sum payable either on death or maturity (after the end of specified period) are also popular. In India, the Pension sector is also handled by Life Insurers.

- **Health Insurance**– The cost of medical expenses has seen a sharp increase in the last few decades. It can cripple the family financially. Health Insurance provides for the cost incurred towards such expenses.
- **Marine, Property, Motor and Miscellaneous Insurance** – The loss caused to the assets is covered under these types of Insurance.

5.2.3 Regulatory Provision Related to Internal Audit and ERM

- **Guidelines on Corporate Governance issued by IRDA**–

Provisions related to Internal Audit, ERM and Internal control are as follows:

Considering the risks that an insurer takes in carrying out its operations, and the potential impact it has on its business, it is important that the Board has in place:

- Robust and efficient mechanisms for the identification, assessment, quantification, control, mitigation and monitoring of the risks;
- Appropriate processes for ensuring compliance with the Board approved policy, and applicable laws and regulations;
- Appropriate internal controls to ensure that the risk management and compliance policies are observed;
- An internal audit function capable of reviewing and assessing the adequacy and effectiveness of, and the insurer's adherence to its internal controls as well as reporting on its strategies, policies and procedures; and
- Independence of the control functions, including the risk management function, from business operations demonstrated by a credible reporting arrangement.

The responsibility for the oversight of control functions of an insurer should be entrusted to Directors possessing the appropriate integrity, competence, experience and qualifications, and they should meet the fit and proper criteria initially and on an on-going basis.

For insurers within a group, appropriate and effective group-wide risk control systems should be in place in addition to the control systems at the level of the insurer. It is essential to manage risks appropriately on a group-wide basis as well.

- **Audit Committee (mandatory)**

- The Audit Committee shall oversee the financial statements, financial reporting and disclosure processes.

- The Chairman of the Audit Committee should be an independent Director of the Board and should ideally be a professional Chartered Accountant or a person with strong financial analysis background. The association of the CEO in the Audit Committee should be limited to eliciting any specific information concerning audit findings.
 - The Audit Committee will oversee the efficient functioning of the internal audit department and review its reports. The Committee will additionally monitor the progress made in rectification of irregularities and changes in processes wherever deficiencies have come to notice.
 - The Audit Committee shall be directly responsible for the appointment, remuneration, performance and oversight of the work of the auditors (internal/statutory/Concurrent). In case of statutory audit, the independence of the external auditors shall be ensured (although the approval of appointment, remuneration and removal of the statutory auditors shall be done by the shareholders at the general body meeting);
 - The Audit Committee shall establish procedures to attend to issues relating to maintenance of books of account, administration procedures, transactions and other matters having a bearing on the financial position of the insurer, whether raised by the auditors or by any other person.
 - Any work other than audit that is entrusted to the auditor or any of its associated persons or companies shall be specifically approved by the Board who shall keep in mind the necessity to maintain the independence and integrity of the audit relationship. All such other work entrusted to the auditor or its associates shall be specifically disclosed in the annual accounts of the insurer.
- **Risk Management Committee (mandatory)**
 - It is now well recognized that the sound management of an insurer

as in the case of other financial sector entities, is dependent on how well the various risks are managed across the organization. In pursuit of development of a strong risk management system and mitigation strategies, insurers shall set up a separate Risk Management Committee to lay down the company's Risk Management Strategy. The risk management function shall be organized in such a way that it is able to monitor all the risks across the various lines of business of the company and the operating head has direct access to the Board. Conventionally this function is under the overall guidance and supervision of the Chief Risk Officer (CRO) with a clearly defined role. The insurers can, however, presently organize the function appropriately to the size, nature and complexity of their business keeping in view the need for operative independence of the Head of the risk management function.

- **Broadly, the Risk Management Committee shall:**
 - Assist the Board in the effective operation of the risk management system by performing specialized analyses and quality reviews;
 - Maintaining a group-wide and aggregated view on the risk profile of the insurer in addition to the solo and individual risk profile;
 - Report to the Board details on the risk exposures and the actions taken to manage the exposures;
 - Advise the Board with regard to risk management decisions in relation to strategic and operational matters such as corporate strategy, mergers and acquisitions and related matters.

5.2.4 Factors That Enhances the Role of IA / ERM And Value-Addition Opportunities

- **Large network of offices-** Insurance business model operates with a large number of offices spread across various geographical locations. Having control over the day to day functioning is not possible for controlling Head Office. It relies on periodical statements sent by the offices. The role of

Internal Audit becomes very crucial for the top management as it requires independent review of the working of these offices.

- **Large number of financial transactions**– Every office of the Insurers undertakes a large number of financial transactions related to business. Strict control over these transactions is required to avoid any chances of misappropriation, fraud and mistakes of critical nature.
- **Regulatory compliances**– Every office of the Insurer is subject to the compliance of large number of Regulatory provisions. The controller has been more and more aggressive on this front to protect the interests of policyholders. Internal Audit plays a vital role in ensuring the Regulatory compliances.
- **Employee Turnover**– Private Insurance sector is prone to large employee turnover. This results into frequent changes in the overall management of the offices of Insurer. Here again, the role of Internal Audit is very important to appraise the management about the effect of such movements on the overall working.
- **Highly technical processes**– Insurance Industry require lot of domain expertise for its functioning. Similarly, the procedures of the Insurance companies are subject to constant review due to the changes in regulations and technology. Internal Audit plays a very important role in suggesting changes in procedures followed by the insurer and any deviation observed in the implementation of procedures and processes.
- **Use of I.T.**– Nowadays, Insurance business is highly automated and uses latest softwares for its operations. Complete review of systems is very critical given the huge amounts invested in I.T. and the extent of dependence on technology.

5.2.5 Critical Segments and Business Areas that can Benefit from IA / ERM

- **Important Areas covered by Internal Auditor in Insurance vis a vis various Departments in Insurance**

➤ **New Business**

New Business department deals with all the functions starting from the receipt of new proposals to the issuance and dispatch of policies to the policyholders

o **Major New Business functions**

- Underwriting of new proposals
- Follow up on pending proposals
- Development of medical network
- Issuance and dispatch of policies
- Control over policy stamps
- Reinsurance Arrangements
- Control over undelivered policies
- Refund of excess deposits in case of cancelled/ rejected/postponed proposals

o **Important areas covered by Internal Audit**

- TAT observed in respect of policy issuance, conveying pending requirements to customer and refund of excess deposits
- Procedure followed for undelivered policies, refund of excess deposits and refund of deposits in respect of cancelled/ rejected/ postponed proposals
- Adequacy of Medical Examiners' network
- Implementation of AML guidelines for all new proposals
- Accuracy and adequacy of supporting documents

collected from the proposer, as per the underwriting manual

- Adequacy of the mechanism for attending to customer complaints in respect of non-receipt of policy documents, forged signatures across proposal forms, third-party cheques, tampered supporting documents, etc.

o **Key Value Additions**

- Compliance with AML guidelines in respect of New Business functions.
- Identification of high risk areas like under-calculation of sum under consideration which will affect decisions pertaining to medical/financial underwriting, reinsurance sessions and KYC documentation.
- Identification of revenue leakages in the form of non-recovery of necessary charges from the refund of excess deposits

➤ **Policy Servicing**

Insurance contract is generally a long-term relationship between the policyholder and the insurer. During the course of contract various types of services are required by the policyholder and such services are provided by the Policy Servicing department.

o **Major policy servicing functions**

- Nomination
- Assignment
- Partial Withdrawal

- Surrender
- Loan
- Fund Switching
- Free look cancellation
- Revival
- Change in Sum Assured
- Change in term
- o **Important areas covered by Internal Audit**
 - Observance of TAT in respect of all policy servicing aspects such as change of nomination, assignment, partial withdrawals, surrender, loan, change of address, fund switching, free look cancellation, renewal etc.
 - Accuracy and adequacy of the supporting documents collected from the policyholder
 - Checking the accuracy of calculations
 - Implementation of AML guidelines as per IRDA guidelines in respect of free look cancellations, surrenders, assignments and renewal
 - Adequacy of the mechanism for attending customer complaints particularly in respect of high-risk areas viz. misrepresentation, wrong selling, frauds, third-party cheques, misuse of policy premium collected from customers, etc.
- o **Key Value Additions**
 - Compliance of AML guidelines for respective policy

servicing functions

- Identification of revenue leakages in the form of non-recovery of necessary charges from surrender/ partial withdrawal/ free look cancellation cases
- Identification of areas of operations which require immediate corrective measures to maintain the standards of policy servicing

➤ **Claims**

Claims department deals with all functions related to registration, processing and admission/ rejection of claims. The major types of claims for life insurers are death, maturity, survival and disability. Whereas in the case of general insurers there are health and other non-life claims.

o **Major Claims functions**

- Registration of claims
- Follow up on pending claim cases
- Development of a network of TPA, surveyors and claim Investigation agencies
- Claim investigations
- Admission and payment of claims
- Repudiation of fraudulent claims

o **Important areas covered by Internal Audit**

- TAT observed in respect of registration of claims, claim settlement, conveying pending requirements to claimants, claim investigation, etc.

- Procedure followed for Claims registration after receipt of claim intimation , follow up with the claimant for pending requirements
 - Adequacy of the investigations carried out in respect of suspicious claims
 - Checking the accuracy of calculations
 - Checking the accuracy and adequacy of the supportive documents as per the Claims Manual and circulars
 - Adequacy of the mechanism for attending to customer complaints in respect of repudiated claims, delayed claim settlement, etc.
- o **Key Value Additions**
- Compliance of AML guidelines in respect of Claims functions
 - Identification of high-risk areas like inadequacy of claim investigations and repudiations not conforming to the provisions of the Claims manual / Insurance Act
 - Identification of revenue leakages due to wrong calculations, wrong selection of risk at the underwriting level, inadequate reinsurance done, etc.
- **Sales Administration**
- Sales administration department deals with the issues related to the Sales force viz. agents, sales managers, branch managers, etc. of the insurer.
- o **Major Sales Administration functions**
- Arrangement of IRDA training

- Licensing of new agents
- Renewal of agents' licenses
- Development of a network of IRDA training institutes
- Commission payouts
- Sales competition payouts
- Appraisal of Sales Manager's performance
- Promotion or demotion or termination of Sales Managers
- o **Important areas covered by Internal Audit**
 - Checking of data related to IRDA training, IRDA examinations, licensing of new agents, renewal of agents' licenses, etc.
 - Adequacy of IRDA training institutes
 - Checking the accuracy of payments made to IRDA training institutes
 - Procedure for termination of and reinstatement of agency
 - Checking the accuracy of commission payouts particularly in respect of Reinstated agents, terminated agents and agents' eligible u/s 44
 - Data-related sales competition for verifying the accuracy of the compilation of eligible agents/ employees' list as per the guidelines of the Scheme circulars
 - Adequacy of the mechanism for attending complaints in respect of non-receipt of commission/ scheme

prizes, non receipt of IRDA licenses, disputes regarding STM Bonuses, promotion criteria, etc.

- Checking of sales promotional expenses, entertainment expenses and sales-related reimbursements

o **Key Value Additions**

- Identification of revenue leakages due to wrong commission payouts, calculation errors in Sales Manager's bonuses, wrong data compilation for competitions, etc.
- Identification of high-risk areas such as licensing without proper documentation, non-supervision of performance of appointed IRDA training institutes

➤ **Finance and Accounts**

All the matters related to General Accounting, Banking, Budgeting and Financial Reporting is taken care by the Finance and Accounts Department

o **Major Finance and Accounts functions**

- Cash and Bank Management.
- Preparation of Financial Statements
- Control over payments made to policyholders, vendors and employees
- Preparation of Budget
- Control over expenses under various accounting heads
- Bank reconciliations

- Submission of the periodical statements sent to higher offices/ IRDA
- o **Important areas covered by Internal Audit**
 - TAT observed in respect of making various payouts, bank reconciliations, submission of the trial balance, etc.
 - Procedures adopted for the deposition of cash in the bank, custody and movement of safe keys and maintaining the safety of the cash counter/ cash box
 - Checking of all cash depositions with DCB and pay-in slips
 - Physical verification of cash, stamps, cheque books and fixed assets
 - Checking of all bank reconciliations
 - Accuracy of the periodical statements sent to higher offices/ IRDA
- o **Key Value Additions**
 - Identification of revenue leakages due to delay in deposition in banks, wrong bank charges, delayed credit by banks, etc.
 - Identification of high-risk areas like
 - 1) Misuse of cash, stamps, etc.
 - 2) Flaws in the maintenance of cash counter/cash box safety
 - 3) Payments made without proper authorization

➤ **General Administration**

All matters related to Office Administration, H.R. and Salary are handled by the General Administration Department.

○ **Major General Administration functions**

- Compliance of the General requirements under applicable labour and industrial acts
- Control over expenses related to general administration such as conveyance, postage, rents, taxes, etc.
- Entering into lease agreements and sales agreements for the offices of the insurer
- Making arrangements with the vendors for the supply of necessary materials required for Office Administration
- Salary administration
- Handling of HR related work such as recruitment, transfers, promotions, retirement, resignation, etc. of the staff.

○ **Important areas covered by Internal Audit**

- Verification of Compliance of the requirements under applicable labour and Industrial acts
- Verification of expenses related to general administration such as conveyance, postage, rents, taxes, etc.
- Verification of lease agreements
- Verification of all the agreements with the vendors

- Salary Payment verification
- **Key Value Additions**
 - Identification of revenue leakages due to
 - 1) Mistakes in calculation of Full and Final settlements, bonus calculations, increments, etc
 - 2) Wrong payments made to vendors
 - 3) Excessive amounts disproportionate to the level of business activity spent under various accounting heads.
 - Identification of areas of high risk such as
 - 1) Lack of control over Leave Records
 - 2) Lack of control over inventory
 - 3) Non-compliance of regulatory requirements with regard to labour and industrial acts

➤ **Actuarial**

Actuarial department deals with jobs related to the mathematical basis of the Insurance.

- **Major Actuarial functions**
 - Development of new Insurance Products
 - Determination of premium tables
 - Valuation of Insurance Business
 - Determination of surplus
 - Maintenance of Solvency Margin

➤ **Investment**

Investment Department deals with the activities related to the Investment of monies collected by the Insurer as per the statutory guidelines.

○ **Major Investment functions**

- Investment of policyholders' fund in accordance with section 27 of the Insurance Act,1938
- Submission of periodical returns to IRDA

➤ **Group Insurance and Pensions**

Group Insurance deals with the policies issued by insurers to a group of persons viz. employees, members of an association, debtors, etc. Contrary to individual insurance policies group insurance policies are tailor-made to cater to the requirements of a group

○ **Major types of group insurance policies**

- Group term insurance
- Group health insurance
- Group gratuity
- Group annuity
- Group saving linked insurance

○ **Important areas covered by Internal Audit**

- Agreement between master policyholder and insurer
- Underwriting of group policies
- Claim settlement under group policies

- Policy servicing
- Accounting of premiums received
- Procedure for entry and exit of members
- Adequacy of data collected from group policyholder
- Calculation of premium
- General accounting
- **Key Value Additions**
 - Indication of revenue leakages due to application of wrong premium tables, allowing entry of new members without fulfilment of minimum insurability conditions, etc
- **IRDA Compliance**
 - Observance of regulations issued by IRDA
 - Formations of various committees as per the IRDA corporate governance guidelines and their functioning
 - Appointment and functioning of various officers as per IRDA guidelines
 - Submission of periodical returns to IRDA

5.3 Depository Participant

5.3.1 Introduction

A Depository is an institution that holds securities in electronic (dematerialised) form and facilitates their safekeeping, transfer, and settlement.

- **Depositories in India**

- NSDL (National Securities Depository Limited)
- CDSL (Central Depository Services (India) Limited)

A Depository Participant (DP) is a SEBI-registered intermediary that acts as a link between an investor and a securities depository (such as NSDL or CDSL) for holding and transacting in financial securities electronically. Investors cannot open a demat account directly with the depository and hence, they open it through a DP.

5.3.2 Role of a Depository Participant:

A Depository Participant acts as an agent of a depository (such as NSDL or CDSL in India) that enables investors to

- Open and maintain Demat accounts
- Hold securities in electronic form
- Transfer securities during buy/sell transactions
- Investor grievance handling

Depository Participant is like a bank branch for shares. Just as a bank holds your money, a DP holds your shares and securities in electronic (demat) form.

5.3.3 Regulatory Framework

A Depository Participant (DP) operates within a well-defined regulatory framework to ensure safety, transparency and efficiency in the securities market. In India, it is primarily governed by the Securities and Exchange Board of India (SEBI) along with the depositories such as National Securities Depository Limited and Central Depository Services Limited.

- **Important Laws:**

The operations of Depository Participants (DPs) are regulated by the Securities and Exchange Board of India under the Depositories Act, 1996 and SEBI (Depositories and Participants) Regulations, 2018, with regulatory

powers derived from the SEBI Act, 1992.

➤ **Depositories Act, 1996:**

- Dematerialization of securities
- Functioning of depositories and DPs

➤ **Securities and Exchange Board of India Act, 1992:**

- Establishes SEBI as a regulator
- Gives authority to SEBI to supervise DP

● **Relevant Regulatory References:**

➤ **SEBI (Securities and Exchange Board of India)**

- SEBI (Depositories and Participants) Regulations, 2018 it is the main governing law for DPs (registration, eligibility, duties, inspections).
- SEBI Act, 1992 empowers SEBI to regulate the securities market and protect investors.
- SEBI Circulars including KYC norms, AML/PMLA compliance, cybersecurity, grievance redressal, and operational instructions.

➤ **NSDL (National Securities Depository Limited)**

- Business Rules of NSDL mention detailed operational procedures for DPs.
- Operational Guidelines / Circulars issued periodically for compliance and system updates.
- DP Operating Instructions (NSDL) states step-by-step procedures for daily DP activities.

- **CDSL (Central Depository Services Limited)**
 - CDSL Operating Instructions detailed rules for handling demat accounts, transfers, pledges, etc.
 - Circulars and communiqués updates on compliance, system changes, and investor services.
 - DP Master Circulars (CDSL) mentioning operational guidelines for DPs.

5.3.4 Registration and Eligibility

- A DP should be registered with SEBI under the SEBI (Depositories and Participants) Regulations.
- Net worth requirements must be maintained (as prescribed by SEBI and depositories).
- Eligible entities include Banks, Financial Institutions, Stockbrokers and Custodians

5.3.5 Compliance and Operational Guidelines

- KYC norms (Know Your Customer) and Anti-Money Laundering rules
- Periodic reporting to SEBI, NSDL/CDSL
- Maintenance of records
- Cybersecurity and data protection standards
- Investor grievance redressal mechanisms

5.3.6 Important Areas covered in Depository Participant and key review points:

Sr. No.	Areas	Key Review Points
1	Account Opening & KYC Compliance	<ul style="list-style-type: none"> ● Check that PAN, Aadhaar, and address proof are valid and match the applicant's details.

Sr. No.	Areas	Key Review Points
		<ul style="list-style-type: none"> ● Confirm the client's identity through an in-person verification process. ● All required customer onboarding details to be mentioned in the prescribed Account opening form. ● Ensure all necessary agreements are correctly filled, signed, and documented. ● Obtain and verify the customer's FATCA self-declaration for tax compliance purposes.
2	Client Master Maintenance	<ul style="list-style-type: none"> ● Ensure all client information is correct, complete, and up to date. ● Update client records promptly whenever changes are required. ● All modifications are approved by authorized personnel before updation.
3	Demat & Remat Requests	<ul style="list-style-type: none"> ● Ensure all required fields in the Dematerialization Request Form (DRF) / Rematerialization Request Form (RRF) are properly filled and valid. ● Verify that share certificates are genuine and correctly submitted. ● Confirm the transposition form is accurately filled when there is a change in the joint holder order. ● Ensure all processing steps are completed within the prescribed time limits.
4	Delivery Instruction Slips (DIS) Control	<ul style="list-style-type: none"> ● Ensure Delivery Instruction Slip booklets are issued ● Confirm that signatures on instructions match the registered client signatures. ● Process all instructions promptly within the required time frame.
5	Transaction Processing	<ul style="list-style-type: none"> ● Check that all transactions are correctly recorded. ● Confirm that trades are settled accurately with no errors. ● Ensure all transactions are approved by authorized personnel.

Sr. No.	Areas	Key Review Points
		<ul style="list-style-type: none"> ● Match and verify all daily records to ensure consistency and accuracy.
6	Pledge transactions	<ul style="list-style-type: none"> ● Verify creation, closure, and invocation requests are correctly processed. ● Ensure all required documents are complete, accurate, and properly filed. ● Confirm that all actions are approved by the designated authorized personnel.
7	Demat Account Closure	<ul style="list-style-type: none"> ● Ensure the account closure form is properly filled and submitted. ● Verify that the signature matches the registered client signature. ● Confirm no securities balance is pending, the account should have nil balance or securities properly transferred before closure ● Verify nominee or legal heir information is correctly recorded and valid.
8	Transmission of Securities	<ul style="list-style-type: none"> ● Ensure the transmission request form is properly filled and submitted. ● Verify the authenticity of the submitted death certificate. ● Check all supporting documents, nominee details, succession certificate / will / legal heir certificate, notarized indemnity (if applicable). ● KYC of the claimant for valid ownership transfer.
9	Investor Grievances	<ul style="list-style-type: none"> ● Maintain proper records and monitor all customer complaints. ● Resolve all complaints within the defined turnaround time. ● Escalation handling for unresolved issues to the higher authority for prompt action.
10	Operational Manual and	<ul style="list-style-type: none"> ● Ensure all DP operations policies and SOPs are formally documented, approved, and periodically

Sr. No.	Areas	Key Review Points
	Policies	updated. <ul style="list-style-type: none"> ● Verify alignment of policies with guidelines issued by SEBI and depositories.
11	Outsourced Activities	<ul style="list-style-type: none"> ● Board Approved Outsourcing policy ● Formal agreement with outsourced vendors ● Intimation to regulators on outsourced vendors
12	DP Service Centres	<ul style="list-style-type: none"> ● Prior approval of the depository for service centres opened and intimation for service centres closed ● Updation of service centres on the depositories website ● NISM certification for associated persons, ● Display of depository services provided at centres.
13	Website-related compliances	<ul style="list-style-type: none"> ● Display information mandated by SEBI/depository on a time-to-time basis ● Investor charter ● Display investor grievance escalation matrix ● Link to the Online Dispute Resolution (ODR) portal ● Link to SCORES
14	Major Policies	<ul style="list-style-type: none"> ● PMLA policy ● Conflict of Interest policy ● Surveillance policy

5.4 Wealth Management

Wealth Management firms are niche service providers within the overall Financial Services domain targeting particularly the HNI and Ultra HNI clients to provide tailored investment advice for creating, preserving and growing their clients' wealth. While niche, it is one of the most rapidly evolving and significantly growing financial service segments in the past few years. This service is particularly opted for planning critical aspects such as retirement, investments, tax strategies, and estate planning.

Wealth Managers provide a wide range of financial solutions to their clients with

the following being the primary domains:

- **Financial planning** – This involves conducting a deep analysis of the risk appetite and investment horizon to achieve the client's long-term investment goals.
- **Investment Management** – Creating a tailor-made portfolio suiting the client's risk profile and financial goals using Alternative Investment Funds, Portfolio Management Services, Mutual Funds, Equity, etc.
- **Estate Planning** – An important aspect of wealth management focusing on creating wills for successfully transferring the wealth to heirs by engaging legal professionals.
- **Tax planning** – Designing strategies and incorporating instruments in the client's portfolio to minimize the tax and maximizing returns.
- **Family Offices** – Wealth management advisory that serves the UHNIs in managing the end-to-end affairs of a family including their personal affairs such as philanthropy.
- **Corporate / Business Advisory** – Assisting clients with cash flow management and personal-corporate financial synergy.

5.4.1 Key regulatory and governing bodies include:

Wealth Management Firms in India operate within a multi-layered regulatory framework. The applicable regulations under various governing bodies are mentioned below:

Governing Bodies	Regulations
Securities and Exchange Board of India	SEBI (Portfolio Managers) Regulations, 2020
	SEBI (Investment Advisers) Regulations, 2013
	SEBI (Mutual Funds) Regulations, 1996
	SEBI (Alternate Investment Fund) Regulations, 2016
	Prevention of Money Laundering Act & KYC Rules

Governing Bodies	Regulations
Reserve Bank of India	Master Circular on Para-banking Activities
	Foreign Exchange Management Act (FEMA) & LRS Guidelines
Insurance Regulatory and Development Authority of India (IRDAI)	IRDAI (Insurance Brokers) Regulations, 2018
	IRDAI (Licensing of Corporate Agents) Regulations, 2002
Pension Fund Regulatory and Development Authority (PFRDA)	PFRDA (Point of Presence) Regulations, 2018
Association of Mutual Funds in India (AMFI)	AMFI Code of Conduct & other rules
Others	Companies Act, Income Tax Act / GST /STT, etc.

5.4.2 Important Areas covered and key review points:

Sr. No.	Regulatory/ Domain	Audit Areas	Key Review Points
1	SEBI PMS/ SEBI Investment Adviser	Registration and Net-Worth requirements	<ul style="list-style-type: none"> ● To check the validity of SEBI registration and scope of permitted activities (PMS/IA/Both) ● Review compliance with minimum net-worth requirements and periodic certification filed with SEBI/APMI ● Validate timely renewal in case of no fresh registration
2	SEBI PMS/ SEBI Investment Adviser	Client Onboarding and Documentation	<ul style="list-style-type: none"> ● Review the client agreement to check if all relevant clauses requiring public disclosures are duly covered ● Check whether a separate annexure of fee is signed by the client and whether an illustrative fee structure is available ● Verify whether the suitability assessment, and adequate risk profiling is completed by the client before commencement of services.

Sr. No.	Regulatory/ Domain	Audit Areas	Key Review Points
3	SEBI PMS/ SEBI Investment Adviser	Fees	<ul style="list-style-type: none"> ● Check the alignment of the fee structure disclosed in the client agreement with the disclosure document and both are well within the defined regulatory limits. ● Transactional testing for incorrect billing, duplicate charging, or non-permitted expenses ● Review maker-check and public disclosures controls over distributor commissions/trail commission, if any.
4	SEBI PMS/ SEBI Investment Adviser	Portfolio Construction and Suitability	<ul style="list-style-type: none"> ● Review whether the investment decisions are made based on the client's risk profiling. ● Check if the exposure norms are complied with ● Portfolio Diversification requirements as per DD and the investment restrictions are factored in ● Ensure deviations to the model portfolio are documented, approved, and disclosed to clients in quarterly client communications.
5	SEBI PMS/ SEBI Investment Adviser	Performance Reporting and Disclosures	<ul style="list-style-type: none"> ● Conduct benchmarking comparison within periodic performance reports sent to clients ● Validate the methodology of valuation and the consistency of the adopted methodology. ● Whether unrealized gains/losses are duly disclosed ● Review marketing material shared with clients. Ensure that no statements that are misleading in

Sr. No.	Regulatory/ Domain	Audit Areas	Key Review Points
			nature or pose selective performance claims are published
6	SEBI PMS/ SEBI Investment Adviser	Governance and Compliance	<ul style="list-style-type: none"> ● Check the appointment, independence, and reporting structure of the Compliance Officer ● Check whether the internal audit is periodically presented to the audit committee of the board and is conducted by a certified professional ● Review minutes for oversight and SEBI communications filed.
7	RBI – Distribution / Agency Business	Manufacturer/ Agency onboarding	<ul style="list-style-type: none"> ● Verify a formal arrangement and valid SLA agreement exists for each manufacturer (MF/Insurance/NPS) ● Verify that all activities are limited to agency business without risk participation ● Ensure that a formal due-diligence process is undertaken before on-boarding any product
8	RBI – Distribution / Agency Business	Segregation of Duties	<ul style="list-style-type: none"> ● Check proper segregation of duties between front-office, back-office, and client advisory functions. ● Verify the presence of a valid DOA before providing any client advice ● Whether a proper maker-checker mechanism exists
9	RBI – Distribution / Agency Business	Product Approval	<ul style="list-style-type: none"> ● Products distributed by the firm should be duly approved by IRDAI ● Check if a product undergoes a series and hierarchy of approval before being onboarded ● Ensure proper vetting

Sr. No.	Regulatory / Domain	Audit Areas	Key Review Points
10	RBI – Distribution / Agency Business	Sales Process & Disclosures	<ul style="list-style-type: none"> ● Check whether a separate annexure of the fee/ benefit structure and adequate risk disclosures are provided to customers ● Check if surrender, lock in, fees and benefits are aptly explained/ disclosed to the clients.
11	RBI – Distribution / Agency Business	After-Sale Servicing	<ul style="list-style-type: none"> ● Review process for policy servicing, endorsements, and claim assistance ● Review the timely grievance redressal mechanism and reporting as per IRDAI guidelines ● Verify customer requests and grievances are timely closed and duly escalated if not closed.
12	PFRDA – NPS / PoP	Subscriber Onboarding	<ul style="list-style-type: none"> ● NPS account openings are completed within the regulatory timelines ● Verify KYC, FATCA, and subscriber consent are adequately documented ● Review if the applications are timely uploaded to the CRA and acknowledgements are duly provided to the clients.
13	PFRDA – NPS / PoP	Contribution and Reconciliation	<ul style="list-style-type: none"> ● Review if the contributions are timely remitted to the CRA. ● Reconcile the client and CRA records
14	AML / KYC	Customer Due Diligence/ Enhanced Due Diligence	<ul style="list-style-type: none"> ● Verify completeness of client-onboarding application. ● Check whether AML and KYC requirements are complied with ● Review of exceptions tracking in the client onboarding process ● Check controls around Enhanced Due Diligence for HNI/PEP/high risk clients

Sr. No.	Regulatory / Domain	Audit Areas	Key Review Points
			<ul style="list-style-type: none"> ● Check source of funds/wealth documentation ● Verify periodic AML/CFT training conducted for employees and record retention ● Board oversight on AML risk assessment
15	AML / KYC	Transaction Monitoring, STR Reporting	<ul style="list-style-type: none"> ● Review alerts generated and investigated for suspicious transactions. ● Timely filing of STRs/CTRs with FIU IND

5.5 Asset Management

5.5.1 Regulatory Framework

An Asset Management Company (AMC) in India operates within a multi-layered regulatory framework, primarily shaped by SEBI's Mutual Fund and AIF Regulations along with Association of Mutual Funds of India (AMFI) rules. **The applicable key rules and regulations are mentioned below:**

- SEBI (AIF) Regulations
- SEBI Master Circular on AIF
- SEBI (Mutual Funds) Regulations & Master Circular
- SEBI Listing Obligations and Disclosure Requirements (LODR)
- SEBI Insider Trading Regulations
- Prevention of Money Laundering Act & KYC Rules
- AMFI Code of Conduct & other rules
- Other Rules & regulations as applicable (Income Tax Act / GST /STT)

5.5.2 Important Areas covered in AMC and key review points

Sr. No.	Areas	Key Review Points
1	Investment Management & Decision Making	<ul style="list-style-type: none"> ● Defined Investment philosophy and its adherence across all schemes ● Review of due diligence process prior to execution of trade transaction ● Controls at the Portfolio diversification level ● Investment Committee Approvals & maintenance of adequate documentation trails. ● Monitoring of fund manager biases and concentration risk pertaining to individual investors.
2	Investment Limit Monitoring	<ul style="list-style-type: none"> ● Investments conditions / limits checks and reporting including leverage calculation ● Review of the operational process of investment execution including allocation of costs / management fees across investors ● Review of process and approvals around early termination of the scheme ● Review of the process around launching a new offshore strategy and adherence to its related compliances
3	NAV Computation & Fund Accounting	<ul style="list-style-type: none"> ● Nav Calculation & maker checker controls ● Valuation policy adherence ● Controls over expense accrual & booking ● Error Tracking & Impact analysis of NAV errors
4	Dealing Room Controls	<ul style="list-style-type: none"> ● Controls over Front Running / insider trading indicators ● Controls over the Trade Execution process ● Controls over Off-Market Transactions
5	Risk Management Framework	<ul style="list-style-type: none"> ● Early Warning Systems for credit downgrades

Sr. No.	Areas	Key Review Points
		<ul style="list-style-type: none"> ● Independence of Risk function from Investment Team ● Stress Testing and Scenario Analysis
6	Expense Management & TER controls	<ul style="list-style-type: none"> ● Total Expense calculation (TER) & its compliance with limits ● Expense allocation over various schemes ● Review of chargeable & non – chargeable expenses ● Disclosure of expenses to investors
7	Custody Level Controls	<ul style="list-style-type: none"> ● Reconciliation between AMC, Custodian and Fund accountant ● Appropriate Segregation of Duties across schemes ● Corporate Actions processing accuracy & due credit to investors
8	Compliance & Regulatory Adherence	<ul style="list-style-type: none"> ● Compliance with all the applicable regulations, guidelines, directions, etc. ● Timely filing of regulatory returns and submissions ● Compliance Testing Controls
9	Product Lifecycle & Governance Controls	<ul style="list-style-type: none"> ● NFO (New Fund Offering) approval process and documentation ● Periodic review of scheme performance vs peers ● Product suitability analysis
10	Investor Servicing & Operations	<ul style="list-style-type: none"> ● Controls over Transaction processing (subscription, redemption & switches) ● Adherence to cut time off & NAV applicability ● Accuracy & timeliness of statement of accounts shared with investors ● Process of handling Investor/distributor grievances.

Sr. No.	Areas	Key Review Points
		<ul style="list-style-type: none"> ● Turnaround time (TAT) monitoring and SLA adherence
11	Broker Empanelment & Review Controls	<ul style="list-style-type: none"> ● Controls present at the time of Broker Empanelment ● Controls over the periodic review framework for brokers ● Controls present to avoid concentration risk for brokers
12	Distributor & Channel Management	<ul style="list-style-type: none"> ● Empanelment & due diligence of distributors ● Commission structure & trail fees validation ● Controls over the mis-selling of various products ● Controls over payments made to Distributors ● Controls in case of distributor claw-backs.
13	Financial Reporting Controls	<ul style="list-style-type: none"> ● Review of revenue recognition principles adopted (Management fees and Performance fees) ● Controls over Related Party Transactions ● Expense Provisioning & accruals
14	Client Onboarding	<ul style="list-style-type: none"> ● Client onboarding verification for completeness of application. ● Verifying AML, KYC requirements are complied with applicable regulations ● Review of the process around exceptions tracking in the client onboarding process ● Review of relevant approvals for personnel reviewing the exceptions.
15	Back Office Controls	<ul style="list-style-type: none"> ● Controls over password sharing between front office & back office personnels ● Deployment of separate personnel between the front office and the back office
16	Investment Bank Accounts	<ul style="list-style-type: none"> ● Bank reconciliation performed ● Identification of idle funds and its deployment

Sr. No.	Areas	Key Review Points
17	Non – Performing Investments	<ul style="list-style-type: none"> ● Controls over the classification of non – performing investments ● Controls over income recognition for non-performing investments ● Controls over appropriate provisions for non performing investments
18	Inter Scheme Transfer	<ul style="list-style-type: none"> ● Controls over due diligence procedure performed to transfer securities from one scheme to another. ● Transfer of securities within respective schemes is carried out with appropriate approvals ● Documentation for such transfer is being maintained

5.6 Retail and Institutional Broking

5.6.1 Regulatory Framework

Stock broking falls under the regulatory ambit of the Securities and Exchange Board of India (SEBI). The applicable key rules and regulations are mentioned below:

- SEBI (Stock Brokers) Regulations, 2026
- SEBI Master Circular for Stock Brokers
- Stock Exchange rules, regulations and bye-laws
- Stock Exchange circulars

5.6.2 Important Areas covered for stock broking and key review points

Sr. No.	Areas	Key Review Points
1	Registration norms	<ul style="list-style-type: none"> ● Availability of valid registration ● Payment of Fees on a timely basis ● Adherence to minimum net worth norms

Sr. No.	Areas	Key Review Points
2	Operational Activities	<ul style="list-style-type: none"> ● Review of Margin Maintenance and monitoring activity ● Review of information flow of clients to exchanges ● Review of submission of periodic statements/reports to clients ● Review of client fund routing process ● Review of an instance of client/error code modification
3	Dealing	<ul style="list-style-type: none"> ● Review of Order acceptance and execution process ● Maintenance of Order placement proofs ● Access controls for the dealing room ● Implementation and adherence to order limits ● Usage of trading terminals at approved locations ● Restriction on the usage of mobile phones
4	Regulatory Compliance	<ul style="list-style-type: none"> ● Adherence to stock exchange bye-laws ● Filing of periodic returns with stock exchanges ● Appointment of Designated Director and Compliance Officer ● Compliance with NISM certification norms for employees ● Periodic Employee Training Programmes ● Availability of suitable insurance cover
5	Financial Reporting	<ul style="list-style-type: none"> ● Verification of Brokerage charged to client ● Collection and payment of various statutory fees, charges and taxes for each trade
6	Surveillance Activities	<ul style="list-style-type: none"> ● Implementation of adequate systems for surveillance of trading activities

Sr. No.	Areas	Key Review Points
		<ul style="list-style-type: none"> ● Adoption of approved Policies and Procedures ● Implementation of appropriate thresholds for the generation of alerts ● Review and updation of systems, processes and control procedures on a periodic basis ● Adequate systems for the detection of mule accounts or suspicious activity ● Implementation of Whistle Blower Mechanism
7	Proprietary Trading	<ul style="list-style-type: none"> ● Availability of stock exchange permission ● Disclosure of proprietary trading to clients ● Adherence to stock exchange limits
8	Investor Onboarding	<ul style="list-style-type: none"> ● Obtention of adequate KYC documents ● Adherence to PML guidelines ● Sharing of Welcome Kit with Investors ● Communication of Most Important Terms & Conditions ● Compliance with Investor Onboarding timelines
9	Investor Grievances	<ul style="list-style-type: none"> ● Availability of designated personnel for grievance redressal ● Resolution of grievances with specified timelines ● Disclosure of client complaints on a monthly basis
10	Disclosures	<ul style="list-style-type: none"> ● Disclosure of policies and procedures on the company website ● Display of license, notices and other information at the premises
11	Contract Note	<ul style="list-style-type: none"> ● Issuance of Contract note on a timely basis ● Adherence to the format prescribed by SEBI and stock exchanges

Sr. No.	Areas	Key Review Points
12	Algorithmic Trading	<ul style="list-style-type: none"> ● Obtention of stock exchange approvals for various algos ● Implementation of Order-level risk controls ● Compliance with order-to-trade ratios ● Adherence to Order Routing norms ● Conducting system audits on half-yearly basis
13	Miscellaneous	<ul style="list-style-type: none"> ● Implementation of Cyber Security and Cyber resilience framework ● Maintenance of compliance calendar ● Maintenance of demat accounts under various categories ● Adherence to the classification of Inactive/Dormant accounts ● Revocation of mobile numbers as per the MNRL list

5.7 Investment Banking

5.7.1 Regulatory Framework

Investment Banker assists the banking, financial services and Insurance sector in facilitating financial advice and raising funds. It acts as an intermediary between the Parties which has capital requirements and those who are willing to invest it. The applicable rules and regulation which governs the Investment banking business as listed below,

- Securities and Exchange Board of India (Merchant Bankers) Regulations 1992
- SEBI Master Circular on Merchant Bankers (September 26, 2023)
- SEBI (Prohibition of Insider Trading) Regulations, 2015
- Indian Prevention of Corruption Act 1988

- Guidelines on Outsourcing of Activities by intermediaries
- Companies Act, 2013
- Prevention of Money Laundering Act & KYC Rules
- General Laws (Contract Law, Tax Law)

5.7.2 Important Areas covered in Investment Banking and key review points

Sr. No.	Areas	Key Review Points
1	Type of Deals	<ul style="list-style-type: none"> ● Merger & Acquisition ● Private equity capital Raising ● Public Issue (IPOs, Rights Issue, Preferential Issue) ● Qualified Institutional Placement (QIPs) ● Bond Issuance ● Securitization
2	Client Due Diligence Procedure	<ul style="list-style-type: none"> ● Client Identification, Risk Categorization (High, Medium, Low) ● KYC Documents as per checklist ● Beneficial Owner Declaration ● Record Keeping & Retention ● Periodic Updation of KYC
3	Client Engagement	<ul style="list-style-type: none"> ● Details of Transactions ● Fee Mechanism ● Indemnification & confidentiality ● Legal Vetting of Engagement letter
4	Regulatory Compliance and Reporting	<ul style="list-style-type: none"> ● Timeliness and accuracy of reporting ● Details of the Compliance officer ● Deficiency and non-compliance ● Track record of past issues. ● Changes in KMP

Sr. No.	Areas	Key Review Points
5	Public Disclosure	<ul style="list-style-type: none"> ● Track record of performance of public issues. ● Offer Documents ● Investor charter based on the categories (For e.g. IPO, FPO, Rights issue, Delisting, Buyback) ● Redressal of Investor Grievance
6	Outsourcing of Activities by Merchant Banker	<ul style="list-style-type: none"> ● Outsourcing risk Management program ● Record Management ● Due diligence & Monitoring performance of third Party. ● Contractual agreement covering Material aspects. ● FIU Reporting
7	Code of Conduct to regulate trading and the prohibition of Insider Trading	<ul style="list-style-type: none"> ● Restriction on trading by a person in possession of Unpublished price sensitive Information ● Maintenance of Chinese walls ● Grey List/Restricted list of stock of Live deals
8	Finance	<ul style="list-style-type: none"> ● Computation of transaction value as per the agreement ● Tax Computation ● Invoice Management ● Delegation of Authority

5.8 Fintech Platforms

5.8.1 Regulatory Framework:

Fintech companies operate under multiple regulatory guidelines depending on their business model (payments, lending, wealth tech, etc.). These regulations ensure financial stability, consumer protection, and secure digital transactions.

Key regulations include:

- Reserve Bank of India (RBI) Act, 1934
- Payment and Settlement Systems Act, 2007
- Information Technology Act, 2000
- Prevention of Money Laundering Act (PMLA), 2002
- Companies Act, 2013
- Digital Lending Guidelines issued by RBI
- Master Directions on KYC (RBI)
- NPCI Guidelines (for UPI and payment systems)
- Data Protection & Privacy regulations (IT Rules)

5.8.2 Important Areas covered in FINTECH platforms and key review points:

Sr. No.	Areas	Key Review Points
1	Customer Onboarding (KYC & Account Opening)	<ul style="list-style-type: none"> ● Compliance with RBI KYC guidelines (CKYC, Aadhaar-based KYC, etc.) ● Validation of customer identity and address proof ● Screening against sanctions/PEP lists ● Timely activation of customer accounts/wallets ● Monitoring of incomplete or pending KYC cases
2	Transaction Processing (Payments / Transfers)	<ul style="list-style-type: none"> ● Accuracy and completeness of transaction processing (UPI, wallets, cards) ● Timely settlement with banks and payment networks ● Monitoring of failed/reversed transactions ● Reconciliation of transactions with settlement accounts

Sr. No.	Areas	Key Review Points
		<ul style="list-style-type: none"> ● Controls to prevent duplicate or unauthorized transactions
3	Lending Operations	<ul style="list-style-type: none"> ● Adherence to RBI digital lending guidelines ● Transparent disclosure of interest rates, fees, and charges ● Proper credit underwriting models and risk scoring ● Monitoring of loan disbursement and repayment cycles ● Collection practices and recovery processes
4	Revenue Recognition	<ul style="list-style-type: none"> ● Proper recognition of revenue streams (commissions, MDR, interest income, fees) ● Verification of revenue-sharing agreements with partners ● Accurate accounting of cashback, discounts, and incentives ● Reconciliation of revenue with transaction data
5	Fraud Risk & Transaction Monitoring	<ul style="list-style-type: none"> ● Real-time fraud detection mechanisms (AI/Rule-based systems) ● Monitoring suspicious transactions and unusual patterns ● Implementation of AML (Anti-Money Laundering) controls ● Reporting of suspicious transactions (STRs) to FIU-IND ● Segregation of duties and approval workflows
6	Data Security & Privacy	<ul style="list-style-type: none"> ● Compliance with the IT Act and data protection norms ● Encryption of sensitive customer data ● Access controls and role-based permissions

Sr. No.	Areas	Key Review Points
		<ul style="list-style-type: none"> ● Regular vulnerability assessments and penetration testing ● Incident response mechanism for data breaches
7	Technology & System Controls	<ul style="list-style-type: none"> ● System uptime and availability (SLA adherence) ● Backup and disaster recovery mechanisms ● Change management controls (for system updates/releases) ● Integration controls with banking partners and APIs ● Audit logs and system traceability
8	Regulatory Compliance	<ul style="list-style-type: none"> ● Valid licenses (NBFC, Payment Aggregator, PPI, etc.) ● Compliance with RBI/NPCI circulars and guidelines ● Periodic regulatory reporting and filings ● Adherence to KYC/AML norms ● Internal compliance monitoring framework
9	Customer Grievance Redressal	<ul style="list-style-type: none"> ● Mechanism for handling customer complaints ● Timely resolution as per regulatory timelines ● Escalation matrix and nodal officer appointment ● Maintenance of complaint registers and tracking system ● Customer communication and transparency
10	Partner / Vendor Management	<ul style="list-style-type: none"> ● Due diligence of third-party service providers ● Agreements with banks, NBFCs, and payment gateways ● Monitoring service level agreements (SLAs)

Sr. No.	Areas	Key Review Points
		<ul style="list-style-type: none"> ● Risk assessment of outsourcing arrangements ● Data sharing and confidentiality controls
11	Treasury & Fund Management	<ul style="list-style-type: none"> ● Maintenance of escrow/nodal accounts as per RBI guidelines ● Daily reconciliation of funds ● Monitoring liquidity and fund flow ● Restrictions on use of customer funds ● Interest handling (if applicable)
12	Marketing & Customer Acquisition	<ul style="list-style-type: none"> ● Transparency in advertisements and promotions ● Compliance with fair practices code ● Verification of referral/affiliate payouts ● Monitoring of customer acquisition costs ● Avoidance of misleading claims
13	Financial Reporting & Accounts	<ul style="list-style-type: none"> ● Accuracy of financial statements ● Reconciliation of bank balances and platform data ● Proper classification of expenses and revenues ● Verification of provisions (loan losses, refunds, etc.) ● Compliance with accounting standards
14	Digital Wallet / PPI Operations	<ul style="list-style-type: none"> ● Compliance with RBI guidelines for Prepaid Payment Instruments (PPI) ● Limits on wallet balances and transactions ● Segregation of customer funds in escrow accounts ● Monitoring inactive/dormant wallets ● Controls over wallet loading and redemption
15	ESG & Ethical Practices	<ul style="list-style-type: none"> ● Responsible lending practices (avoidance of

Sr. No.	Areas	Key Review Points
		<p>over-indebtedness)</p> <ul style="list-style-type: none"> ● Transparency in algorithm-based decisions (credit scoring, approvals) ● Fair treatment of customers and non-discriminatory practices ● Environmental and social risk considerations (if applicable) ● Ethical use of customer data
16	Investor Reporting & Governance	<ul style="list-style-type: none"> ● Accuracy and timeliness of MIS/shared reports to investors ● Compliance with shareholder agreements ● Monitoring KPIs like CAC, LTV, NPA ratios, etc. ● Board reporting and governance structure ● Transparency in disclosures to stakeholders

RSM India



Mumbai (Corporate Office)

96-97, 9th Floor,
Maker Chambers VI,
Nariman Point, Mumbai – 400021

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, B-37, Sector 1,
Noida – 201 301

Gurugram

407, Time Tower, Sector 28, MG
Road, Gurugram – 122002

Chennai

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

Bengaluru

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

Hyderabad

1208, Gowra Fountainhead,
Huda Techno Enclave, Hitec City,
Hyderabad – 500 081

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

101/102, 1st Floor, UDB Tower
University Marg, Bapu Nagar
Jaipur- 302 015

Vijayanagar

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

For further information please contact:

RSM Astute Consulting Pvt. Ltd.

301-307, 3rd Floor, Technopolis Knowledge Park, Mahakali Caves Road, Chakala, Andheri East, Mumbai 400 093.

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/RSMIndia



x.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 presents an overview of internal audit practices in the BFSI sector, with a focus on leveraging automation, analytics, and artificial intelligence. 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.

May 2026

© RSM India, 2026