What are the key areas that demand Internal Audit attention?

March 2025

The better the question. The better the answer.
The better the world works.

Shape the future with confidence

1 Cybersecurity

By 2025, a global study predicts that software supply chain attacks will have affected 45% of organizations worldwide, marking a significant increase of three times compared to 2021. Risks associated with the use of cyber-physical systems and IoT, open-source code, cloud applications, complex digital supply chains, social media, and more have brought organizations' exposed surfaces outside of a set of controllable assets.

In light of this, the Audit Committee may want to consider five crucial elements when determining the coverage of internal audits.

01

Adequacy of the cybersecurity framework and comprehensiveness of cyber risk assessment program:

- Identification of "Crown Jewels"
- Alignment to frameworks like NCRF, NIST, ISO 27001, PCIDSS, etc.
- Review pertinence/implementation of policies and procedures

02

Effectiveness of the design and operating efficiency of cybersecurity controls:

- Evaluation of control framework
- Assess the integration of controls in the IT environment
- Analyze incident / breach data for root cause

03

Adequate identification and compliance with local and international regulatory requirements:

- Regulations like IT Act/ Rules, NCSP 2013, SPDI rules, etc
- Mechanism to identify gaps or non-compliance
- Sustainable remedial actions

04

Incident response and recovery readiness in terms of availability of right fit of skills, resources and cyber insurance to manage a security breach:

- Sufficient technical resources
- Organizational measures to detect and respond
- Accountability of third-party manned SOC

05

Alignment of critical and integrated supply chain to defined cybersecurity strategy to ensure the company does not fall under the blast radius of an attack on third party:

- Identification of critical supply chain
- Assessment of impact of security breach
- Measures to prevent and recover from impact

2 Data Privacy

According to IBM's Cost of a Data Breach Report 2024*, compiled by the Ponemon Institute, the average global cost of a data breach is US$4.88 million in 2024, compared to US$4.45 million in 2023, with 46% of breaches involving customer data. The average cost of a data breach in India is US$2.35 million in 2024, which is higher than the US$2.18 million reported in 2023. These costs continue to rise and include loss of business, detection and escalation, post-breach response, and regulatory/public notification.

Consequently, there are five key elements that an audit committee could consider for inclusion in the internal audit coverage:

01

Adequacy of the data privacy framework, comprehensive identification of "Personal Data," data classification process and computation of privacy impact assessment

- Framework alignment to regulations like DPDP, CCPA, GDPR, HIPAA, etc
- Review pertinence/implementation of policies and procedures
- Identification of personal data elements along with applicable touchpoints

02

Effectiveness of the design and operating efficiency of data access and protection controls

- Comprehensiveness of personal/sensitive data identification
- Assessment of data storage, retrieval, usage and protection
- Data access controls, audit trail/logging, monitoring and response to breach

03

Adequate identification and compliance with local and international data privacy regulations

- Regulations like DPDP, CCPA/CPRA, GDPR, HIPAA, PCIDSS etc
- Mechanism to identify gaps or non-compliance
- Sustainable remedial actions

04

Ability to manage data breaches and privacy incidents including effectiveness of breach response plan

- Review incident response plan with roles and responsibilities
- Breach response readiness
- Breach notification strategy and post incident learnings in alignment with regulations

05

Adoption of "Privacy by Design" principles and "Data Minimization" practices

- Privacy principles to be inbuilt in new system development
- Collecting only that data required for business purposes
- Training and awareness to business on data collection

3 Responsible AI

According to a CEO survey by EY, while 65% of CEOs acknowledge the efficiency benefits of AI, they also emphasize the urgent need to address its social and ethical risks. HBR reports that 67% of CEOs highlight the integration risks associated with AI, underscoring challenges related to trust and the potential for errors. With the evolving landscape and increased focus on AI, it is crucial to address risks such as biases, ethical concerns and data privacy.

As organizations adopt AI governance frameworks, key elements that an audit committee could consider in internal audit include:

01

Adaptive governance frameworks addressing the new challenges and advancements in AI technology.

- Alignment with EU AI Act, ISO 42001, ISO 23894, etc.
- Review the implementation of policies and procedures
- Validate coverage and completeness including the consideration of fairness, accountability, transparency and ethical use of data

02

Evaluation of AI systems design and impact to address ethical, operational and security risks.

- Assess the effectiveness of AI systems in maintaining data quality, integrity and security
- Evaluate potential consequences of AI deployment, use and misuse on individuals, groups and societies

03

Adequate identification and compliance with local and international regulatory requirements.

- Regulations such as EU AI Act, GDPR or other relevant laws
- Establish mechanisms to identify gaps or non-compliance in AI ethics and take remedial actions

04

Assessing risks and implementing effective risk mitigation strategies

- Evaluate management of organizational AI risks, such as biases, discrimination, privacy and security
- Assess key areas such as design, algorithmic, performance and data risks

05

Assessing third party relationships for procurement of LLMs and AI technologies

- Limit the use of open-source AI systems and software and adopt containerized solutions to enhance security, manageability and scalability
- Ensure robust contracts with third-parties including comprehensive security and privacy clauses

4 Social media management

Engagement on social media is an essential practice for companies in the modern digital landscape as it provides an opportunity to gather market intelligence, stay ahead of industry trends, gain insights into consumer behaviour, preferences and emerging patterns. It allows businesses to keep a pulse on their brand reputation by tracking mentions, comments and feedback across various social platforms. This real-time insight into public perception is invaluable for managing a brand's image and addressing any negative sentiment swiftly before it escalates.

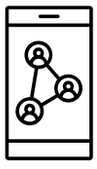
Considering the power of social media, key aspects that an audit committee could consider for inclusion in the internal audit coverage:

01

Availability and adequacy of social media risk assessment framework:

- Comprehensiveness of social media policy including permissible usage
- Clearly defined roles and responsibility including escalation matrix for any events / crisis
- Alignment with cybersecurity and data privacy standards
- Awareness and training programs on social media protocols on a regular basis

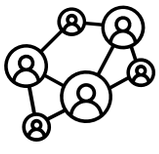
02



Assess procedures in place to initiate, monitor and approve the content creation :

- Availability of clearly defined verbal, style and visual guidelines in compliance with regulatory guidelines
- Evaluate all content creation, approval and publishing as per branding guidelines
- Detection mechanism for misleading content or false claims
- Ensure clearance by branding, marketing and communication team before publishing

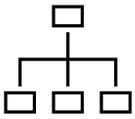
03



Assess framework in place to monitor and manage reputation risks, including responding to negative comments or crises on social media platforms:

- Evaluate the process to detect, categorize and escalate critical / negative comments
- Ensure monitoring and reporting of potential legal concerns around data privacy or defamation
- Response are fact checked, consistent and aligned with official position and timeliness

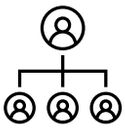
04



Assessment of selection and monitoring process of third-party social media vendor:

- Review alignment with company values and policies
- Adequacy of data-sharing agreements and related regulatory compliances
- Adherence to compliance and security protocols

05



Effectiveness of social media management by the organization:

- Review effectiveness of tools and technologies used for monitoring
- Assess whether relevant metrics are monitored (reach, engagement, sentiment analysis) and are reported to management regularly

5 ESG and Sustainability

As per a World Economic Forum* report, based on scenarios developed by an Intergovernmental Panel on Climate Change (IPCC) the most likely trajectory for the planet's rising average temperature is 2.5° to 2.9° celsius over pre-industrial levels by 2050.

Climate change may cause an additional

US$1.1	14.5	US$12.5
trillion in extra healthcare costs	million deaths	trillion in economic losses worldwide

Hence, it is inevitable for companies to move from a regulatory-led to a purpose-led CSR agenda. Accordingly, the following are five key elements an audit committee could consider in an internal audit coverage:

01

Review alignment of ESG strategy with overall business strategy and integration into corporate risk management

- Identification of material ESG issues and its prioritization
- Governance structure in place to oversee
- Reporting practices and performance matrices

02

Adherence with local ESG related laws and regulations and local/ international reporting standards

- Alignment with BRSR, GRI, SASB, UNSDG, etc.
- Mechanism to identify gaps and take remedial actions
- Compliance with laid down policies and procedures

03

Assessment of reliability and transparency of ESG reporting including completeness, accuracy, integrity and consistency of data published across different reporting frameworks

- Evaluation of data sources
- Mechanism to collect data with integrity
- Reporting aligned to requirement of standards

04

Efficacy of programs to assess and manage carbon footprint, reduce GHG emission, transition to low carbon economy, physical risks related to climate change and practices to ensure DEI, human rights and fair working conditions in operations and supply chains

- Review ESG / sustainability initiatives undertaken
- Evaluate the robustness of transition plans
- Assess timelines and milestone achievements

05

Effectiveness of stakeholders' engagement around ESG / sustainability topics and related trainings

- Identification of stakeholders and prioritization
- Strategies and method of engagement with stakeholders
- Quality and dissemination of training programs

6 Related Party Transactions

Related party transactions ('RPTs') have always been in focus by regulators and other stakeholders. Regulators closely monitor RPTs because they can present risks of conflict of interest, financial manipulation and unfair practices. Companies Act, Income Tax Act, SEBI, Listing Agreement, RBI etc in multiple regulations / circulars / forums have re-emphasised the need to identify and thoroughly scrutinize related or connected party transactions. Regulators have strengthened the mechanism with an aim to enhance transparency, improve quality of information to investors and expand the scope of reporting by companies/ auditors.

Accordingly, the following key elements could be considered by the Audit Committee in internal audit coverage:

01

Governance and adequacy of the related party framework policy:

- Identification and classification of related parties viz subsidiaries, affiliates, KMP, family members etc.
- Business rationale and purpose of transaction to validate legitimate business interest
- Policies and procedure for conflict of interest management

02

Effectiveness of the design and operating efficiency of internal controls and risk assessment:

- Adequacy of segregation of duties and authority matrix around transaction initiation and its contracting
- Assessments of defined preventative and detective controls
- Comprehensive evaluation of the systems/ ERP deployed for recording / tracking transactions

03

Fairness of pricing and terms of transactions:

- Pricing of RPT's are at arm's length by benchmarking against market prices
- Ensuring agreed terms and other conditions are consistent with prevailing market terms
- Assessment of profitability to analyze financial burden of these transactions, if any

04

Adequate identification and compliance with local laws and advisory issued by regulators such as:

- Regulations like Companies Act, Income Tax act, SEBI LODR and other related notifications
- Alignment with regulatory reporting and disclosure considerations to SEBI, MCA, etc.
- Adequacy of disclosure in financial statements

05

Evaluation of ongoing monitoring program:

- Ensuring transactions are within the approved approval limits
- Any changes or deviations are identified and reported to audit committee / board
- Actions are initiated to address whistleblower complaints or for any breach of contract

7 Subsidiary governance by parent company

Corporates create subsidiary companies for a variety of strategic, operational and financial reasons. By establishing subsidiaries, a parent company can diversify its business activities, enter new markets or focus on specialized services without affecting its core operations. Subsidiaries also allow companies to isolate financial and legal risks, as liabilities are often limited to the subsidiary itself. This structure provides flexibility in tax planning, as subsidiaries may operate in regions with favourable tax laws, helping optimize the overall tax burden.

Subsidiary governance is crucial for both integral and non-integral subsidiaries to ensure alignment with the parent company's values, strategic objectives, policies and procedures, and regulatory compliance. For integral subsidiaries, which are tightly linked to the parent company's core operations, effective governance helps maintain operational consistency and mitigates risks that could impact the entire organization. For non-integral subsidiaries, strong governance ensures that these entities operate independently yet still adhere to corporate standards, reducing potential reputational and legal risks for the parent company. This governance framework enables the parent company to oversee and control subsidiaries effectively, supporting sustainable growth and shareholder trust. Accordingly, key elements an Audit Committee of the parent company could consider in the internal audit coverage:

01

Governance associated with the subsidiary to ensure financial, operational, compliance and strategic risks are identified and managed:

- Level of delegation and adequacy of monitoring by parent on key decisions
- Identification of key risks that have an impact on parent company
- Alignment of the risk profile of the subsidiary with the overall risk management strategy of the holding company
- Alignment with parent company's digital strategies and road map

02

Adherence to all relevant local and international laws and regulations:

- Assess the effectiveness of the compliance programs
- Identify any areas of potential non-compliance
- Compliance with SEBI guidelines on corporate governance, as applicable, and / or impact of NFRA recommendation on subsidiary management / governance

03

Internal control system are in place to safeguard assets, ensure the reliability of financial reporting and promote efficient operations:

- Assess entity level controls are designed appropriately and operating effectively
- Alignment with parent company's standards and objectives
- Control gaps, if any, are identified and adequately addressed
- Monitoring mechanism of risks and status of corrective actions

04

Accuracy and timelines of the subsidiary's financial reporting:

- Financial statements prepared are accurate, complete and in accordance with applicable accounting standards and Companies Act 2013
- Reflects true financial position
- Align with parent company's consolidation requirements

05

Monitoring of transactions between the subsidiary and parent company or within subsidiaries:

- Transactions conducted at arm's length
- Recorded timely and accurately
- Compliance with transfer pricing / Companies Act / other regulations

8 Business Continuity Plan (BCP) and Disaster Recovery (DR)

Our 2024 CEO Confidence Index highlights CEOs increasing focus on business continuity and resilience considering geopolitical, technological and economic risks. CEOs are updating business continuity plans (BCP) and disaster recovery (DR) strategies to address new challenges, to enable companies stay resilient against market disruptions. The EY CEO Imperative series emphasizes that companies prioritizing BCP and DR are better positioned to handle risks like supply chain disruptions and regulatory shifts. Additionally, the EY 2022 CEO Outlook survey underscores the role of advanced technology in strengthening operational resilience, helping organizations scale and recover effectively.

In today's volatile environment, its essential that organizations have robust BCP and DR plans in place. Key elements that an audit committee could consider in internal audit include:

01

Comprehensive risk assessment:

- Evaluate risks associated with business applications, operations, data security and third-party services that may affect continuity of operations.
- Review strategies for mitigating risks that could disrupt business continuity, such as natural disasters, cyberattacks and system failures.
- Assess the potential impact of various disruption scenarios on critical business functions and recovery timelines.

02

Adaptive governance frameworks for BCP and DR:

- Ensure alignment with global standards like ISO 22301 for BCP and ISO 27031 for DR.
- Regularly review and update BCP and DR policies to reflect changes in business operations and emerging threats.
- Ensure plans address all critical business applications and areas, including data security, operational processes and recovery timelines.

03

Evaluation of BCP and DR effectiveness:

- Assess the organization's ability to maintain critical operations during disruptions, ensuring minimal downtime.
- Evaluate the results of regular testing and crisis simulations to confirm that BCP/DR procedures are effective and adaptable.
- Ensure that essential data remains secure, accessible and recoverable during incidents.

04

Regulatory compliance and risk mitigation:

- Ensure that the organization complies with relevant laws, such as data protection regulations, information security regulations which may have specific continuity and recovery requirements.
- Identify potential gaps in BCP and DR processes that could expose the organization to operational or legal risks during a disruption.

Our Offices

Ahmedabad
22nd Floor, B Wing, Privilon
Ambli BRT Road, Behind Iskcon Temple
Off SG Highway, Ahmedabad - 380 059
Tel:+ 91 79 6608 3800

8th Floor, Building No. 14A
Block 14, Zone 1
Brigade International Financial Centre
GIFT City SEZ
Gandhinagar – 382 355, Gujarat
Tel: + 91 79 6608 3800

Bengaluru
12th & 13th Floor
"UB City", Canberra Block
No.24 Vittal Mallya Road
Bengaluru - 560 001
Tel:+ 91 80 6727 5000

Ground & 1st Floor
11, 'A' wing
Divyasree Chambers
Langford Town
Bengaluru - 560 025
Tel:+ 91 80 6727 5000

3rd & 4th Floor
MARKSQUARE
#61, St. Mark's Road
Shantala Nagar
Bengaluru - 560 001
Tel:+ 91 80 6727 5000

1st & 8th Floor, Tower A
Prestige Shantiniketan
Mahadevapura Post
Whitefield, Bengaluru - 560 048
Tel:+ 91 80 6727 5000

Bhubaneswar
8th Floor, O-Hub, Tower A
Chandaka SEZ, Bhubaneswar
Odisha – 751024
Tel: + 91 674 274 4490

Chandigarh
Elante offices, Unit No. B-613 & 614
6th Floor, Plot No- 178-178A
Industrial & Business Park, Phase-I
Chandigarh - 160 002
Tel:+ 91 172 6717800

Chennai
6th & 7th Floor, A Block,
Tidel Park, No.4, Rajiv Gandhi Salai
Taramani, Chennai - 600 113
Tel:+ 91 44 6654 8100

Delhi NCR
Aikyam
Ground Floor
67, Institutional Area
Sector 44, Gurugram - 122 003
Haryana
Tel: + 91 124 443 4000

3rd & 6th Floor, Worldmark-1
IGI Airport Hospitality District
Aerocity, New Delhi - 110 037
Tel: + 91 11 4731 8000

4th & 5th Floor, Plot No 2B
Tower 2, Sector 126
Gautam Budh Nagar, U.P.
Noida - 201 304
Tel:+ 91 120 671 7000

Hyderabad
THE SKYVIEW 10
18th Floor, "SOUTH LOBBY"
Survey No 83/1, Raidurgam
Hyderabad - 500 032
Tel:+ 91 40 6736 2000

Jaipur
9th floor, Jewel of India
Horizon Tower, JLN Marg
Opp Jaipur Stock Exchange
Jaipur, Rajasthan - 302018

Kochi
9th Floor, ABAD Nucleus
NH-49, Maradu PO
Kochi - 682 304
Tel:+ 91 484 433 4000

Kolkata
22 Camac Street
3rd Floor, Block 'C'
Kolkata - 700 016
Tel:+ 91 33 6615 3400

6th floor, Sector V,
Building Omega, Bengal Intelligent Park,
Salt Lake Electronics Complex, Bidhan Nagar
Kolkata - 700 091
Tel: + 91 33 6615 3400

Mumbai
14th Floor, The Ruby
29 Senapati Bapat Marg
Dadar (W), Mumbai - 400 028
Tel:+ 91 22 6192 0000

5th Floor, Block B-2
Nirlon Knowledge Park
Off. Western Express Highway
Goregaon (E)
Mumbai - 400 063
Tel:+ 91 22 6192 0000

3rd Floor, Unit No.301
Building No.1, Mindspace-Gigaplex
IT Park, MIDC, Plot No. IT-5
Airoli Knowledge Park
Airoli West, Navi Mumbai - 400 708
Tel: + 91 22 6192 0003

18th Floor, Altimus
Pandurang Budhkar Marg, Worli
Mumbai - 400 018
Tel: + 91 22 6192 0503

Pune
C-401, 4th Floor
Panchshil Tech Park, Yerwada
(Near Don Bosco School)
Pune - 411 006
Tel: + 91 20 4912 6000

10th Floor, Smartworks
M-Agile, Pan Card Club Road
Baner, Pune - 411 045
Tel: + 91 20 4912 6800

Ernst & Young LLP

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EYG member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/en_in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at Ground Floor, Plot No. 67, Institutional Area, Sector - 44, Gurugram - 122 003, Haryana, India.

SA1

ey.com/en_in

@EY_India EY EY India EY Careers India @ey_indiacareers