REDEFINING INTERNAL AUDIT: A FRESH PERSPECTIVE FOR UNPRECEDENTED TIMES

ADITYA SANGHVI
Student - Global Risk Management Institute

Abstract

The traditional role of internal audit, focused on compliance and controls, is no longer sufficient in today's dynamic and rapidly changing world. This article argues that internal auditors must evolve into strategic risk navigators, actively identifying and mitigating threats that could jeopardise an organisation's existence.

Introduction

The business landscape is experiencing constant disruption driven by technological advancements, economic shifts, and geopolitical uncertainties. Internal audit functions must adapt to this new reality by moving beyond traditional practices and embracing a strategic perspective focused on mitigating critical risks that can make or break an organisation.

> "We always overestimate the change that will occur in the next two years and underestimate the change that will occur in the next ten. Don't let yourself be lulled into inaction."
>
> ~ Bill Gates

The world is in a state of flux. Technological advancements are happening at breakneck speed, economies are constantly evolving, and geopolitics throws curveballs with alarming regularity. In this dynamic landscape, the role of the internal auditor can no longer be confined to the traditional realm of checklists, controls, and ensuring compliance. A fresh perspective is needed – one that positions internal audit as a strategic partner, actively mitigating risks that threaten an organisation's very existence.

> *According to a Harvard Business School Professor in the book The Balance Scorecard:* ***"Translating Strategy into Action, 90% of organisations fail to execute their strategies successfully. However, some say that 95% of strategic plans fail."***

From Compliance to Strategy: A Shift in Focus

Traditionally, internal auditors have excelled at identifying operational risks, compliance gaps and IT vulnerabilities. These remain crucial functions, but they are no longer enough. The future of internal audit lies in its ability to address strategic risks. These risks, broadly categorized as external and internal, can make or break an organisation. Statistics suggest that companies that are not able to address strategic risks on time have disappeared or significantly reduced their market share.

- External Strategic Risks: These stem from factors outside the organisation's control, such as:
  - Failure to adapt to disruptive technologies: Imagine a company clinging to outdated brick-and-mortar retail models while the Quick Commerce revolution unfolds in India. They risk losing market share if they don't leverage this new channel to reach customers.
  - Economic downturns: A global recession or pandemic can wreak havoc on unprepared businesses.
  - Shifting geopolitical landscapes: Regulatory changes or trade wars can disrupt entire industries.
- Internal Strategic Risks: These stem from decisions made within the organisation, such as:
  - Poor decision-making: A bad acquisition or a flawed product launch can have disastrous consequences.
  - Compromising quality for cost savings: Cutting corners on materials or safety can lead to product recalls and reputational damage.
  - Failure to innovate or monetize intellectual property: Companies that fall behind the innovation curve are at risk of being overtaken by competitors.

Real-life Risk posed by Quick Commerce Companies to Traditional Retail and e-commerce companies.

In India, quick commerce players like Zepto, Blinkit and Swiggy Instamart are not restricting themselves to groceries, essentials and utilities. They have started delivering consumer electronics including iPhones that are delivered to customers in under 5 – 10 minutes. Imagine the risk they are posing to traditional retail as well as traditional E-commerce companies. According to a 2024 report from , the quick commerce (q-commerce) market in India was valued at $652 million in 2023 and is expected to reach $19,932.5 million by 2030, with a compound annual growth rate (CAGR) of 63%.

Bridging the Gap: The Internal Auditor as a Strategic Risk Navigator

So, how can internal auditors equip themselves to tackle strategic risks? Here's a roadmap:

Understanding the Big Picture: Internal auditors need to move beyond individual processes and departments. They must grasp the organisation's overall goals and objectives, and assess how each audited area aligns with the strategic vision.

Asking the Right Questions: During audits, the focus should shift towards facilitating discussions about strategic risks. For example, in the Quick Commerce scenario, an internal auditor might ask: "Has the management explored strategic partnerships with Quick Commerce companies to expand reach?" The management's response and proposed mitigation strategies become crucial insights.

Elevating the Conversation: The audit committee meetings should become a platform for in-depth discussions about strategic risks. This ensures that these critical issues reach the highest levels of management.

Beyond the Checklist: Expanding the Internal Audit Toolkit

To become effective strategic risk navigators, internal auditors need to expand their skillsets beyond traditional auditing practices. Here are some additional areas of expertise to consider:

- **Data Analytics:** Data analysis is crucial for identifying hidden patterns and trends that could indicate emerging risks. Mastering data analysis tools will empower auditors to extract valuable insights from vast data sets.
- **Scenario Planning:** The ability to forecast potential future scenarios, and assess their likelihood and impact, will allow auditors to proactively identify potential strategic risks and recommend contingency plans.
- **Industry Knowledge:** Staying abreast of industry trends and disruptive technologies specific to the organisation's sector allows auditors to anticipate potential challenges and opportunities.
- **Communication Skills:** Effectively communicating complex risks to non-technical stakeholders is paramount. Internal auditors need to translate their findings into clear, concise, and actionable insights for the management to understand.

Emerging Threats: The Expanding Risk Landscape

The traditional focus on financial risks alone is no longer sufficient. In today's world, internal auditors must also consider:

- **Cybersecurity Risks:** With increasing reliance on technology, cyberattacks pose a significant threat. Assessing an organisation's cybersecurity posture and identifying vulnerabilities are essential internal audit functions.
- **Third-Party Risks:** Partnerships with external vendors can introduce new vulnerabilities. Internal audits need to evaluate the risk profiles of third-party vendors and ensure proper controls are in place.
- **ESG Risks:** Environmental, Social, and Governance (ESG) issues are becoming increasingly important for investors and consumers. Internal audits should assess an organisation's ESG practices and identify potential areas for improvement.
- **Futuristic Risks:** As technologies like AI, ML, Robotics, RPA & Blockchain evolve, internal auditors need to stay informed about their potential risks and opportunities for the organisation.
- **Changing Consumer Preferences:** As consumers are more informed and have an abundance of data, they are making conscious decisions while making their purchases. For instance, they consider buying healthier products or a product which is produced using sustainable practices or from a brand that showcases care for its customers and society.

Taming the Hydra: Insights for a Spectrum of Futuristic Risks

Use case of "A.I. & Intelligent Automation in TPRM"

AI can be used to segment the vendors into High-risk, medium-risk and low-risk.

Automated relevant questionnaires could be made and sent to the vendors after review.

For screening, AI can scrape through different reputed portals and analyse the risk profile, negative news, previous offences or pending litigations and sanctions.

For continuous monitoring, there can be a dashboard for high to medium-risk vendors who are critical from the Perspective of AML, ABAC, Data privacy, Cyber security, BCP DR, and Supply Chain which brings in alerts for emerging risks faced by the vendor.

If there is serious risk posed by the vendor, the system should automatically trigger alternative vendor discovery if needed and should bring new competitive quotes for the same. As the TPRM life cycle for onboarding a customer like in the case of banks can be as long as 6 months, certain repetitive processes can be automated. For continuous monitoring, AI can be the best Use case (also helpful in overall supply chain risk and triggers).

Use of AI-based contract terms analysis & AI-based contract formation which can address the typical risk faced and mitigating measures that create a favourable and win-win contract taking into consideration all aspects and scenarios.

Use of advanced search techniques on search engines, use of advanced scrapping tools to gather data about third parties and analyse them to navigate the risks.

Use case of "A.I. & Intelligent Automation in Cyber Security"

- Technologies are emerging that will monitor threats in real time and also mitigate them. There are tools which not only monitor networks, applications, cloud and endpoint devices for threats and malware but also provide a comprehensive report to mitigate those threats and vulnerabilities. Internal Audit can make use of such reports and escalate them for timely resolution.
- Future is not far where AI can also do secure code reviews more efficiently than any humans can.

Use case of "AI/ML, blockchain and NLP for Data Loss Prevention"

- Advanced Threat Detection: AI/ML algorithms can analyse user behaviour, data access patterns, and content to identify anomalies that might indicate a potential data breach. This allows for a more proactive approach to DLP, focusing on the riskiest activities.

- Content Classification: AI can be trained to automatically classify sensitive data with greater accuracy than traditional rule-based systems. This ensures that only truly sensitive information is flagged for potential DLP violations.
- User Entity and Behaviour Analytics (UEBA): UEBA leverages AI to analyse user behaviour patterns, entity relationships, and context to identify suspicious activity that might indicate a DLP attempt. It analyses a wider range of user activities and contextual information to identify unusual behaviour that could indicate a data exfiltration attempt. For example, a sudden spike in file downloads or emailing sensitive documents to personal accounts could trigger an alert.

Natural Language Processing (NLP)

NLP can be used to analyse the content of emails, messages, and documents in real time, identifying keywords or phrases that indicate sensitive information being shared inappropriately. This can be particularly helpful in detecting attempts to mask sensitive data through techniques like data obfuscation.

Blockchain

While still in its early stages of adoption for DLP, blockchain has the potential to create tamper-proof audit trails for data access and movement. This can provide a more secure and transparent way to track data and identify potential leaks.

Use case of “A.I. Surveillance & Sensors”

- Industries can augment AI surveillance systems in high-risk environments like in an oil & gas Industry, manufacturing plants prone to accidents and mishaps, warehouses with high-value goods or high-tech robots, hazardous chemicals, ATMs and branches of banks etc. These systems can be trained to trigger during specific events, suspicious activity and manage the movement of the goods, people and robots. These systems can also alert stakeholders, and give warnings in multiple relevant languages to prevent or be alert in a certain event or activity.
- Prevent suspicious activity and physical activity in the server rooms and vicinity.
- These systems can also be used to control the quality of goods and filter damaged or sub-standard goods.
- Produce more informed reporting and decision-making.

Use case of “Blockchain-based audit trail, especially in Banking and Financial Services Industry”

- Blockchain technology has the potential to revolutionize the way audit trails are maintained especially for the banks and financial services industry, where each record is crucial and any manual unauthorized changes can pose critical risk to the organisation.
- Blockchain-based changelogs also offer greater security to the overall sensitive data.

Use case of “AI & ML in Fraud Detection and Anomalies in Data”

- AI & ML can analyse the data and trigger data anomalies and suspicious data patterns which can be helpful in uncovering frauds.
- This tech can be used for real time “Transaction Monitoring & Suspicious Transaction Reporting” for AML complainces.
- Internal auditors can leverage predictive analytics to become more proactive. By analysing past data on fraud, errors, inefficiencies, and risks, auditors can build models to predict future issues

  1. Focus on high-risk areas: Prioritize areas most likely to have problems, saving time and resources.

  2. Prevent issues: Shift from identifying problems to predicting and preventing them.

  3. Make data-driven decisions: Use insights to allocate resources and mitigate risks more effectively.

  Scenario: Credit Card Fraud Detection

  AI/ML Method: Machine learning models are trained on historical data containing legitimate and fraudulent transactions. The model analyzes various factors like:

  - Transaction amount
  - Location and time of transaction
  - Merchant category
  - User's past purchase history

  Anomaly Detection: The model learns to identify normal spending patterns for each user. When a new transaction deviates significantly from the user's typical behaviour (e.g., a large purchase from a geographically distant location), it's flagged as suspicious.

Use case of “RPA in Internal Audit, Cyber and Cloud Security”

Internal Audit:

- **Data Extraction and Aggregation:** RPA bots can efficiently extract data from various sources, such as ERP systems, CRMs, and financial databases. This eliminates manual data entry and reduces the risk of human error.
- **Transaction Testing:** Automating repetitive transaction testing allows auditors to focus on exceptions and analyse potential anomalies.
- **Reconciliation Tasks:** RPA can streamline account reconciliations, comparing data sets from different systems and highlighting discrepancies for further investigation.
- **Compliance Testing:** Automating compliance testing processes can ensure consistent adherence to internal controls and regulations.
- **Report Generation:** RPA can automate the generation of standard audit reports, saving time and ensuring consistency in formatting and presentation

Cloud Security Applications:

- **User Provisioning and Access Management:** RPA can automate user account creation, modification, and deletion in cloud environments. This ensures timely access for legitimate users while minimizing the risk of unauthorized access.
- **Security Patch Management:** RPA bots can automate the process of identifying, downloading, and installing security patches across various cloud-based systems. This reduces the risk of vulnerabilities being exploited.
- **Activity Monitoring and Log Management:** RPA can automate the collection and analysis of security logs from cloud platforms, helping to identify suspicious activity and potential breaches.

Cybersecurity Applications:

- **Incident Response:** In the event of a cyberattack, RPA can automate routine tasks like isolating compromised systems, notifying relevant personnel, and initiating recovery procedures. This allows security teams to focus on critical incident response activities.
- **Vulnerability Scanning and Remediation:** RPA can automate vulnerability scanning across systems and applications, followed by the deployment of pre-defined remediation steps for identified vulnerabilities.
- **Phishing and Spam Detection:** RPA can be trained to analyze email content and attachments, flagging suspicious messages for further investigation, potentially saving the organisation from phishing attacks and malware infections.
- **Password Management:** RPA can automate password resets and enforce strong password policies, reducing the risk of unauthorized access due to weak credentials.

Use case of "Technology for ESG Wins"

Environment:

- Big Data & Analytics: Analyze energy use, waste to target improvements and guide sustainability efforts.
- LoT Sensors: Monitor resources, and emissions in real-time for proactive environmental impact reduction.
- Blockchain for Circular Economy: Track materials to promote waste reduction and product reuse.

Social:

- AI for Fair Recruitment: Uncover potential biases in hiring practices to promote diversity and inclusion.
- Cloud HCM Software: Streamline employee onboarding, and training for a positive work environment.
- Blockchain for Ethical Sourcing: Track goods to identify labour violations and ensure ethical practices.

Governance:

- RPA for Compliance: Automate tasks like financial reporting, freeing up time for strategic initiatives.
- RegTech Solutions: Automate regulatory compliance processes to reduce errors and fines.
- Data Visualization Tools: Clearly communicate complex ESG data to stakeholders for impactful reporting.

These are just some of the many use cases an Internal Auditor can augment to complement his audit procedures, automate and ensure greater assurance by leveraging this tool. The crux lies in experimenting, learning new technology and tools and exploring different use cases.

Conclusion

- Internal audit needs to prioritize strategic risks over operational ones, focusing on threats that can significantly impact an organisation's success.
- Internal auditors must broaden their understanding of organisational goals, ask strategic risk-oriented questions during audits, and elevate risk discussions to the highest management levels.
- Expanding the internal audit skillset to encompass data analytics, scenario planning, industry knowledge, communication skills, and expertise in emerging threats like cybersecurity, ESG risks, and futuristic technologies is crucial.
- Utilizing AI, machine learning, blockchain, and other advanced technologies can significantly enhance internal audit capabilities in areas like third-party risk management, cybersecurity, data loss prevention, surveillance, and fraud detection.

Visionary Statement:

Internal auditors have the potential to become invaluable strategic partners within organisations, proactively identifying and mitigating critical risks through a data-driven, technology-augmented approach. By embracing continuous learning and adaptation, internal audit can play a vital role in ensuring the long-term success and resilience of organisations in the face of an ever-changing world.

This vision portrays internal auditors as not just guardians of compliance but as strategic risk navigators who leverage cutting-edge technologies and possess a deep understanding of evolving threats to safeguard organisations and ensure their long-term survival and success.

Citations

CoherentMi. (n.d.). Retrieved from Coherent Market Insights: https://www.coherentmi.com/industry-reports/india-quick-e-commerce-market/market-size

Gates, B. (1996). https://www.inc.com/damon-brown/this-perfect-bill-gates-quote-will-frame-your-next-decade-of-success.html. Retrieved from www.inc.com.

Kalpan, R. S. (1996). The Balanced Scorecard: Translating Strategy into Action.