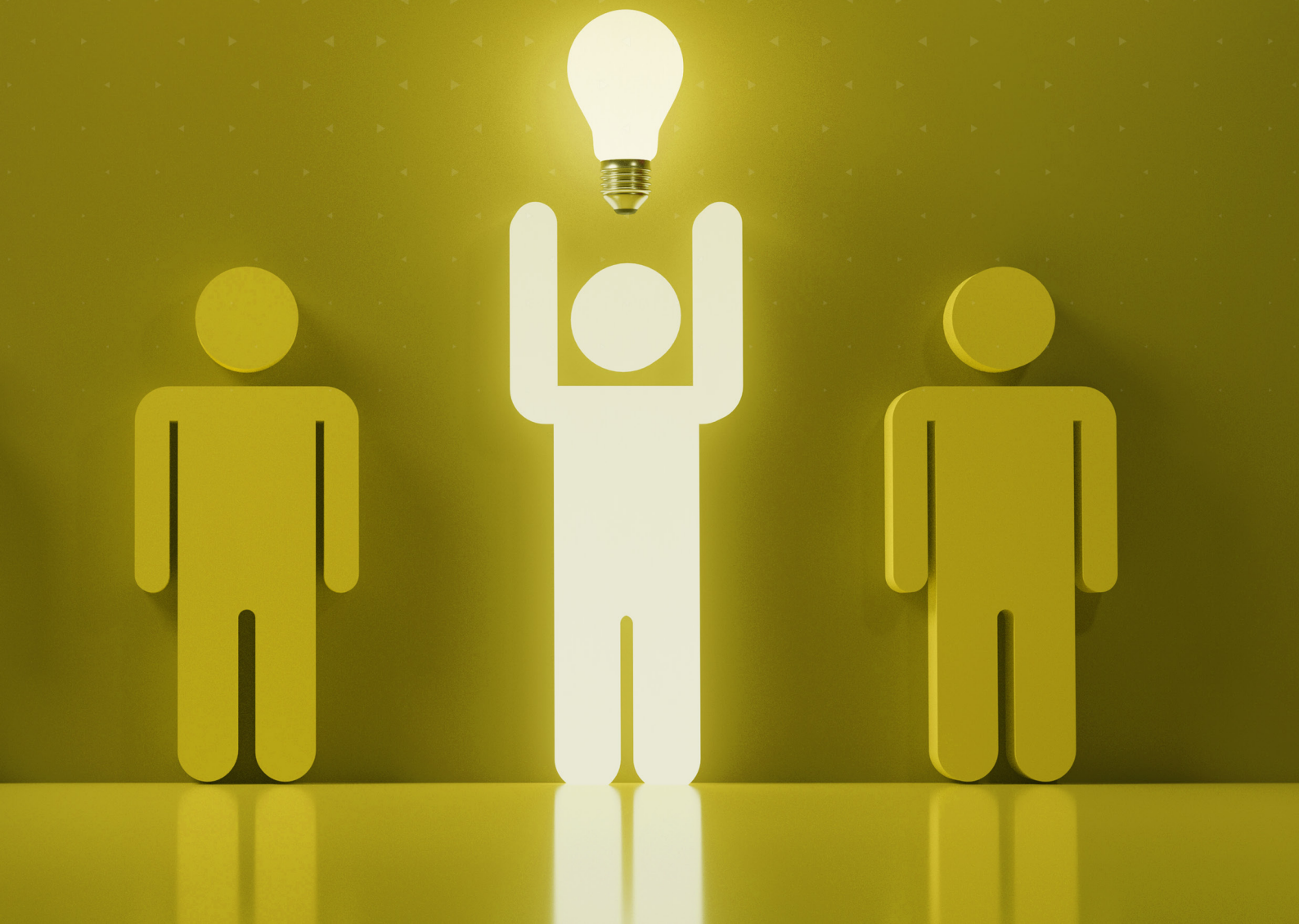
EMERGING MINDS STUDENT'S FORUM



Independence

The Soul of Internal Audit

Anvi Agarwal & Suraj Akolia
Scholar – Global Risk Management Institute (GRMI)

Independence is not just a principle of internal audit. It is the basis of trust that gives each audit opinion its credibility and value.

The internal audit is a function whose objective is to provide independent and objective assurance on the management process of the organization, controls and risk management system. That not only finds the gaps but also advises on future improvements. The value that internal audit generates is based on one key principle, and that is independence.

Lack of independence may result in manipulation of audit findings from management pressure, personal relationships and conflict of interest. These events effect stakeholder confidence. On the other hand, an independent audit function results in greater transparency, accountability and continuous improvement.

The saying "Independence: The Soul of Internal Audit" captures the spirit of the profession. Independence provides the internal audit activity with credibility, integrity and effectiveness, just as the soul brings life and purpose to the human body. Without it, the internal audit becomes a more administrative task than a useful assurance and value-generating activity.

Why Independence Is the Soul of Internal Audit

The primary responsibility of an internal auditor is to evaluate business processes, identify risks and assessing internal controls. In order to perform their duties properly they must be independent of any influence that could hamper their judgement. The independence enables the auditors to provide an honest report on issues identified in the audit, even where results related to the senior management.

Independence is also crucial to maintain a professional scepticism. Internal auditors should not take what the management says to be the truth, they should examine, this will help in detecting fraud,

improve internal controls and reduce organizational risk.

That's why independence is not a checkpoint, it is the base that makes internal audit reliable and trustworthy.

Organizational Independence and Individual Objectivity

Although independence and objectivity are closely related, but they have different meanings.

Organizational Independence

Organizational independence is about the placement of the internal audit function in an organization. For this purpose, to be achieved, the CAE (Chief Auditor) is required to report to the Audit Committee or Board of Directors instead of being subjected to influence or control by the audited department.

In such way, the internal auditors can do their job independently without any management intervention, further they can access any information required for the audit purpose.

Individual Objectivity

The definition of objectivity could be seen in the personal attitude of every internal auditor. The objectives of internal auditor must depend upon his decision-making process that should not affected by the personal bias and conflict of interest.

It is also necessary for an auditor to declare interest that would affect his decision-making process.

Organizational independence offers the correct setting while individual objectivity allows an auditor to utilize that independence correctly.

Independent Auditors' Threats and Safeguards

Though independence is significant on its own accord, many factors can determine the extent of independence if this independence is not protected in an appropriate manner.

In the case where these protection and safeguard measures are consistently applied, then the internal auditors will conduct themselves independently without any form of influence and interference

Price of absence of Independence

The ramification of loss of auditor independence could be devastating. When auditors are being influenced by the management or self-interest sets in, there are high chances that some significant risks will be overlooked. That results in financial damage, monetary sanctions, building negative reputation and loss of stakeholder trust.
For organizations that fail to provide for auditor independence, there will be a lot of governance problems since decision-makers will lack dependable and impartial information. It will not only be limited to financial loss it will also affect business continuity.

Independence into the Organizational Culture

The maintenance of independence of auditors should be done not only by the internal auditing department but the entire organization. The creation of an organizational culture based on integrity, openness, and accountability will ensure that internal auditors will be able to do their work without any hindrance. The BOD, the Audit Committee, senior management, and employees play their significant part in establishing such organizational culture.

This culture can be achieved by encouraging employees having free and open communication, valuing the opinion of the internal Auditor on issues,

looking at results of audit as tool for development does not blame. Leaders should exemplify for ethical behaviour, avoid interfering in audit tasks and protect auditors from retaliation when they report significant issues.

Periodical ethics training, a strong whistleblower process, and clear policies on conflicts of interest further make strong foundation for culture of independence. If independence becomes an integral part of the value system of the organization, then internal audit will be in a better position to provide assurance and contribute to stability in the organization.

Role of Independence in Corporate Governance

Corporate governance is the system which directs the organization. This is based on transparency, accountability, ethics, and good decision making. The existence of independent internal audit contributes to good corporate governance, since this is an opportunity for getting an impartial evaluation of the organization's governance policy and practice by the Board of Directors and Audit Committee. The reason is that internal auditors are independent and hence they will not be biased while reporting any form of governance deficiency or breach of the organizational policies.

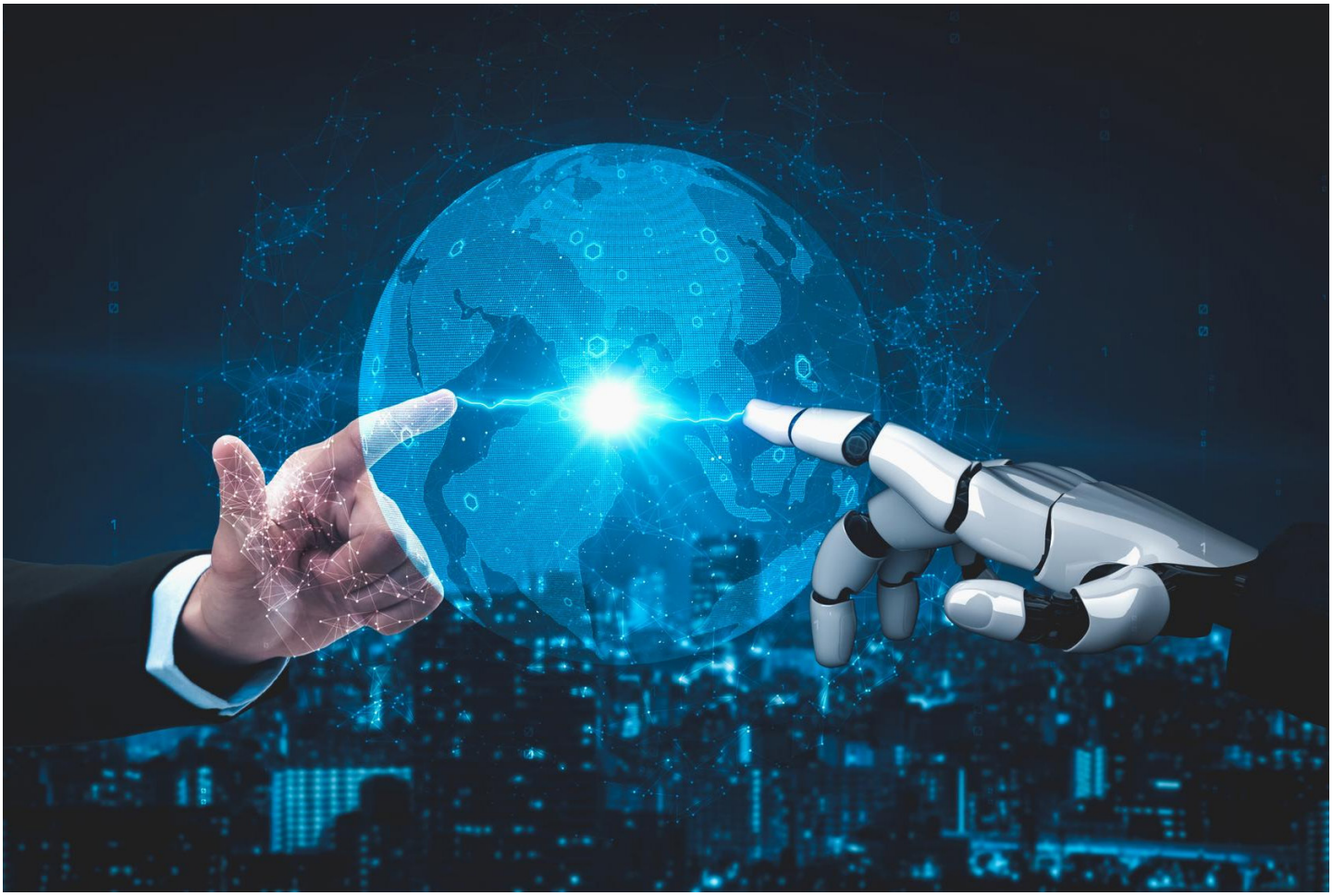
Role of Independence in Managing Risk and Internal Control

Organization faces various type of risks that majorly include financial, operational, technological, legal, and reputational risks. The independent internal audit activity evaluates whether these risks are adequately identified, evaluated, and managed or not and further tasked with assessing the efficiency of internal controls that are established to assure proper financial reporting, achieve operational efficiency, and conform to legal requirements. This is because, being independent in their audits, helps them to detect, control problems and any fraud risks that exist without any bias or outside influence.

Through providing reliable assurance about the efficacy of risk management and control systems, independent internal audit ensures that the organization is stronger and better managed.

Independence in the Era of Artificial Intelligence & Digitalization

Technological advances have evolved the conduct of internal audit activities. Currently, internal auditors use AI, data analytics, automation and other technological methods to examine voluminous information and detect any anomalies. Despite the



usefulness of the above-listed technologies during audit processes, the professional judgment and responsibility of internal auditors should not be replaced by any technologies.

With increasing dependence of firms on technology, new challenges have emerged such as cybersecurity threats, privacy concerns, biasness in algorithms due to which AI governance has become, crucially important and more relevant to the organization. In this regard, it is important that internal auditors keep their independence and autonomy in the process of identifying and assessing risks and not merely an outcome of the use of technology. It is vital that internal auditors do not get overly dependent on the automated system and information from managers without verifying it.

Therefore, in the era of digitalization, technology acts as an essential tool which is used in many areas, but still independence is the basis of credibility in internal audit.

Final Reflection

As discussed in this article, the theme of independence is a key element in all dimensions of internal audit. Independency helps auditors remain objective, handle multiple risks, conflicts of interest, and contribute towards good corporate governance, enhanced risk management, an efficient internal control system, provide transparency and accountability. At the time when Artificial Intelligence and other digital technologies become more and more popular, technology can help auditors in their job, but it will never be able to replace an independent judgment and values of an auditor.

Finally, independence makes internal audit a trustable and valuable adviser rather than a simple routine compliance function work. It ensures that the stakeholders know that audit results are objective, unbiased, honest and oriented towards the benefit of the organization. In other words, without independence, internal audit loses its reputation and credibility while with independence, it gains its reputation and becomes a valuable tool in the protection of the organizational value. That's why independence is not just a principle of internal auditing it is truly the soul of the profession.

No Fear, No Favour

Why Internal Audit's Independence Is Non-Negotiable

Pratik Das & Parnita Singh
Scholar – Global Risk Management Institute (GRMI)

The Flaw in the Watchdog's Collar

In October 2001, Arthur Andersen was a towering member of the Big Five accounting firms, a global empire built on trust with 85,000 employees. By the summer of 2002, the firm was effectively dead. It wasn't destroyed by a market crash or a bad investment; it was obliterated by a conflict of interest.

While auditing the energy giant Enron, Andersen wasn't just checking the books—they were also pocketing roughly $27 million a year in consulting fees from them. When Enron's massive, engineered financial fraud began to unravel, the "independent" watchdog didn't bark. Instead, they spun up the paper shredders, destroying thousands of pages of audit documents to protect their client.

Similar disasters have played out worldwide, like the Satyam scandal in India, where auditors repeatedly failed to verify basic cash balances that turned out to be completely fabricated.

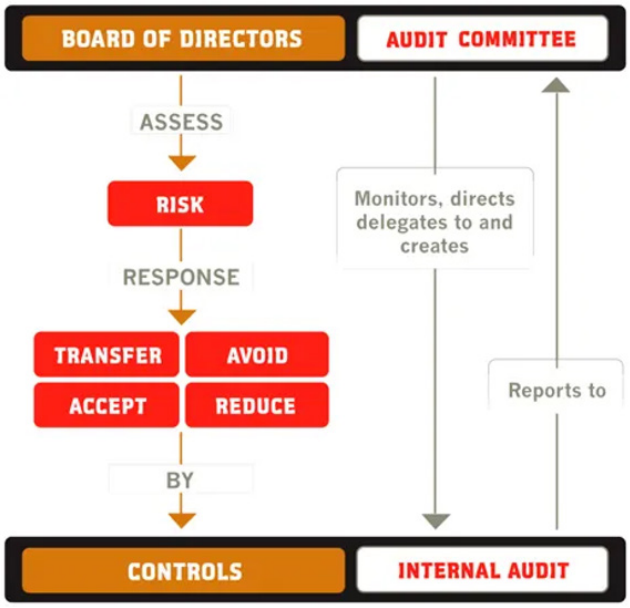
The Central Paradox These collapses exposed a systemic flaw at the heart of corporate governance, forcing a vital question that the financial world still struggles to solve: Can an auditor truly be independent when they answer to—and are paid by—the very people they are supposed to watch?

Independence of internal auditor

Internal audits play a significant role in the company's growth by ensuring that the company is moving in the right direction. Therefore the internal auditor should be given independence in his work so that the objectives of the organization can be achieved. In many of the scams the internal auditors are charged for not finding frauds and taking preventive steps in collusion with the top ranking officers.

Independence implies that judgment of a person is not subordinate to the wishes or directions of another person who might have engaged by him, or to his own self interest. The internal auditors shall safeguard him to mitigate the risk arising

from such circumstances and relationships relating to the threat of independence. Independence is embedded in the definition of internal auditing as it is referred to as an 'independent and objective assurance activity'. One of the core principles states that Internal Audit is 'objective and free from undue influence' i.e. is 'independent'. Attribute standard 1100 states that the 'internal audit activity must be independent and internal auditors must be objective in performing their work.'



Types of independence

There are three main ways in which the auditor's independence can manifest itself-

- **Programming independence** - This independence essentially protects the internal auditor's ability to select the most appropriate strategy when conducting an audit. Auditors must be free to approach a piece of work in whatever manner they consider best. As a client company grows and conducts new activities, the internal auditor's approach will likely have to adapt to account for these. In addition, the internal auditing profession is a dynamic one, with new techniques constantly being developed and upgraded which the internal auditor may decide to use. The strategy/proposed methods which the auditors intend to implement cannot be inhibited in any way.

- **Investigative independence** - While programming independence protects auditors' ability to select appropriate strategies, investigative independence protects the auditor's ability to implement the strategies in whatever manner they consider necessary. Basically, auditors must have unlimited access to all company information. Any queries regarding a company's business and accounting treatment must be answered by the company. The collection of audit evidence is an essential process, and cannot be restricted in any way by the client company.

- **Reporting independence** - Reporting independence protects the auditors' ability to choose to reveal to the public any information they believe should be disclosed. If company directors have been misleading shareholders by falsifying accounting information, they will strive to prevent the auditors from reporting this. It is in situations like this when auditor independence is most likely to be compromised.

Common factors that may hinder internal audits

Internal auditors are skilled at identifying risk for the organization but are not immune to risks themselves. Common risk factors affecting the function include talent shortages, remote work, internal relationship dynamics, evolving skill needs, and technology tool gaps.

- **Talent shortages**

Attracting and retaining internal audit staff has become an ongoing capacity challenge for many organizations. Hiring budgets have grown in some cases, but filling open positions remains difficult. Companies need to bring in talent with flexibility around the requirements of today's workforce. Strict rules about facetime and office hours are becoming obsolete and a barrier to recruiting. Instead, emphasize individual growth, learning, and work-life balance.

- **Remote work**

Today's distributed workforce has made internal auditing more complex than ever. Fieldwork that once required a few localized site visits may now require traveling to multiple locations — or conducting interviews entirely by video. On the plus side, teams that are comfortable with remote information gathering can use video conferencing and digital documentation to streamline data collection and lower the time and cost required to support the audit.

- **Relationship barriers**

Distributed workforces have also created relationship barriers across teams. Without informal in-office moments, teams may have fewer trusted relationships to lean on, which complicates some audit conversations and investigations. Fewer touchpoints between audit and stakeholders may require deliberate effort to maintain ties.

- **Evolving skill needs**

While critical thinking has always been core to the auditor's skill set, the supporting skill list is growing quickly. Current needs include risk assessment, cybersecurity, data mining, and analytics expertise. Today's teams also need to stay current on new cyber threats and new technologies — including GenAI tooling and AI governance frameworks like ISO/IEC 42001.

- **Technology solution gaps**

Teams must ensure they have the right technology to do the work. Audit automation centralizes audit management, improves cross-team collaboration, and increases function efficiency. Staying current on integrations and training the team on new tools is part of the discipline.

Safeguarding independence:

Internal auditors must have unrestricted access to all data, information, records, property, personnel, systems and processes, and there should be no interference to scope of work.
The internal audit head must engage directly with the audit committee or the board. If the Chief Financial Officer or another person outside the Internal Audit department delivers the internal audit presentation, it will impair the independence of the internal auditor.

In some organizations, they would like internal audit to have an additional responsibility such as those relating to ethics or risk management. In order to preserve the independence of internal audit, there must be adequate safeguards built into such roles, and prior approval must be obtained from the audit committee or the board. In an in-house internal audit function, independence can be reinforced through the position of the Chief Audit Executive, organization structure and reporting.

Conclusion

There shall be independence in the internal audit work and also the internal auditor should be given much independence except the monitoring on its functions and reporting formalities, so as to achieve the best result to the company and its stakeholders. There shall be no impairments in the independence and objectivity of the internal auditor. This could able to prevent frauds in the present or in future. It is important for the internal audit activity to be free from interference in all stages of the internal audit process - scope of audit, performing work and communicating results. Being independent is a challenge. It surely does not need significant mental or physical effort to overcome.

It needs courage to stand up to what is right. If there is a potential impairment to independence, the internal auditor should fearlessly highlight to senior management or the audit committee and have it resolved. Therefore independence of internal auditor is considered important for having a successful functioning of the business entity.

From Digital Shadows to Digital Trust

How Privacy-by-Design and Data Classification Can Restore Customer Confidence

Tanisha & Yashas
Scholars - Global Risk Management Institute (GRMI)

Abstract

Trust has become a critical business asset in the digital economy. Organizations increasingly depend on personal information to deliver services, personalize experiences, and develop AI-driven capabilities. Yet rising data breaches, extensive digital profiling, and growing concerns regarding transparency have created a significant trust deficit between organizations and consumers. This article argues that the customer trust crisis stems from governance and architectural weaknesses, not only cybersecurity failures. By adopting data classification frameworks, Privacy-by-Design principles, and Privacy-Enhancing Technologies (PETs), organizations can transition from reactive privacy management to proactive digital trust strategies. Drawing on ISACA's Digital Trust Ecosystem Framework (DTEF), COBIT 2019, NIST, and ISO standards, and examining regulatory developments across the European Union, the United States, China, India, and Brazil, the article traces how classification, embedded privacy, and governance together restore customer confidence.

Introduction: The Emerging Trust Crisis

Trust has always been fundamental to economic activity. Historically, it enabled individuals to engage confidently with banks, governments, healthcare providers, and businesses. In today's digital economy, trust has become even more critical. Nearly every interaction generates, stores, or processes personal information. Consumers routinely share sensitive data when shopping online, using mobile banking, accessing healthcare, or engaging with social media. Organizations rely on this information to improve customer experiences, train AI systems, and drive business growth. Yet the expansion of data collection has created profound concerns.

According to Cisco's 2024 Consumer Privacy Survey, 81% of consumers believe privacy practices reflect organizational values, and 76% are unwilling

to purchase from organizations they do not trust with their information. Pew Research findings reveal that nearly 80% of individuals are concerned about how companies use their personal data, while more than 70% believe they have little control over information collection and processing. The Edelman Trust Barometer 2024 adds that only 30% of people worldwide are comfortable embracing AI, while 35% outright reject it. The technology sector, historically the most trusted industry, saw its advantage shrink from roughly 90% of markets in 2016 to about half by 2024.

The financial impact is measurable. IBM's 2025 Cost of a Data Breach Report documented that the average global cost of a data breach reached US$4.44 million, with the U.S. average at $10.22 million. For healthcare and financial services, costs exceeded $9 million per breach. Beyond direct costs, 43% of organizations experienced customer churn following a breach, with recovery requiring two to three years. These concerns have intensified as organizations deploy AI, predictive analytics, and behavioural TTA profiling technologies at scale.

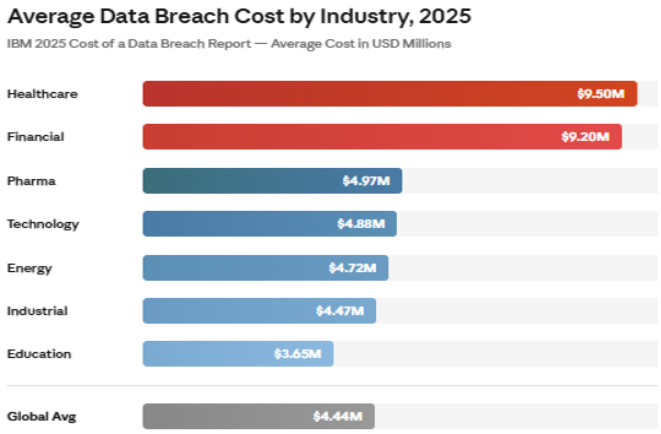


Figure 1: Average Data Breach Cost by Industry, 2025 (IBM)

Table 1: Key Drivers of the Digital Trust Deficit

Driver	Example	Organizational Impact
Data Breaches	Meta, Equifax, Change Healthcare	Reputational damage, regulatory penalties, customer loss
Excessive Collection	Behavioral profiling, digital shadows	Customer mistrust, compliance burden, privacy debt
Lack of Transparency	Complex privacy notices, opaque sharing	Reduced engagement, regulatory escalation
Third-Party Sharing	Advertising ecosystems, data brokers	Accountability gaps, breach exposure multiplication
AI Profiling	Automated decision-making, algorithmic bias	Ethical concerns, regulatory risk, trust erosion

Sources: IBM 2025, Cisco 2024, Edelman 2024, Pew Research

Digital Shadows: The Hidden Cost of Data Transformation

One of the most significant yet least visible consequences of digital transformation is the creation of digital shadows. Every interaction within the digital ecosystem contributes to an expanding repository of information about individuals. Unlike traditional records collected for a specific purpose, digital shadows are continuously generated through routine activities: browsing websites, using mobile applications, engaging with social media, and interacting with connected devices.

IDC projects the global data sphere to exceed 180 zettabytes in 2025, with continued exponential growth thereafter. The world generates approximately 2.5 quintillion bytes of data daily, reflecting the scale of digital interactions. Yet estimates suggest that more than 60% of this data is never analysed and exists primarily to satisfy potential future use cases rather than current business needs. A significant portion of enterprise data remains unused, creating governance and security burdens.

The challenge extends beyond volume. Data initially collected for one purpose may subsequently be used for targeted advertising, recommendation engines, fraud analytics, customer segmentation, AI model training, or third-party partnerships. A consumer purchasing a product online generates dozens of data points: device identifiers, location data, browsing history, payment metadata, and behavioral analytics. As these profiles expand, the distinction between personalization and surveillance becomes blurred. Organizations that collect information simply because it might become useful in the future face asymmetric risk: maximum protection overhead for minimal business benefit.

Why Current Systems Are Failing

Despite significant cybersecurity investments, privacy incidents continue at alarming rates. This suggests organizations are addressing symptoms rather than root causes.

The Data Maximization Problem

For years, organizations operated under a simple philosophy: collect as much data as possible because future business value might emerge. Declining storage costs and advances in analytics encouraged a "collect now, use later" strategy. While this generates business insights, it creates substantial privacy risks. The more information an organization stores, the greater the consequences if that information is compromised. The reality is straightforward: organizations cannot lose data they never collected. Security teams must protect every byte equally, regardless of actual use.

Privacy Debt

Similar to technical debt, privacy debt accumulates when organizations prioritize rapid innovation over responsible privacy practices. It develops through excessive data collection, poor retention management, limited data classification, inadequate privacy assessments, weak third-party oversight, and uncontrolled AI deployments. Privacy debt is particularly dangerous because it remains invisible until an incident occurs. Unlike cybersecurity vulnerabilities that can be identified through technical testing, privacy debt accumulates quietly within organizational processes, databases, and business practices. By the time regulators, customers, or auditors identify the issue, remediation costs can be substantial.

Fragmented Governance

Privacy responsibilities are often distributed across multiple departments. Security teams focus on cyber threats. Legal teams focus on compliance. Business teams focus on growth. Technology teams focus on innovation. Without integrated governance, accountability gaps emerge, leaving privacy risks unidentified until significant incidents occur. COBIT 2019 addresses this through its governance objectives, particularly APO13 (Managed Security) and APO12 (Managed Risk), which require classification and risk assessment as inputs to integrated governance.

Data Classification: The Missing Foundation

Classification means sorting data by how sensitive it is, how critical it is to the business, and what rules apply to it. It sounds basic. In practice, many organizations skip it or do it poorly, and downstream privacy controls and trust mechanisms end up with nothing solid to stand on. ISACA's COBIT 2019 framework treats classification as an input to both security controls (APO13) and risk assessment (APO12), making it a governance prerequisite.

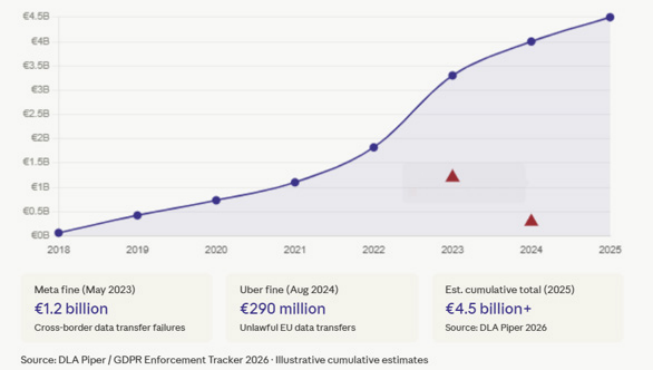
Table 2: Key Frameworks for Data Classification

Framework	Scope	Classification Approach
FIPS 199	U.S. federal systems; impact-based categorization	Low / Moderate / High impact on CIA
NIST SP 800-60 Rev. 2	Federal info types; updated for AI, cloud, IoT	Information category + confidentiality impact
ISO 27001:2022 A.5.12	International; lifecycle-wide classification	Based on CIA + legal requirements
China GB/T 43697-2024	National standard; cross-border transfers	General / Important / Core Data tiers
DOJ EO 14117 Rule	U.S. sensitive personal data; bulk transfers	6 categories + volume thresholds
EU AI Act	AI systems in EU market; high-risk training data	Unacceptable / High / Limited / Minimal risk
COBIT 2019 APO13/APO12	Enterprise governance; security and risk	Classification as input to controls + risk assessment

Sources: NIST, ISO, Chinese SAC, DOJ, EU, ISACA

What has changed recently is the shift from voluntary guidance to legal mandate. China's Data Security Law imposes a three-tier system backed by GB/T 43697-2024. In the United States, the DOJ's Final Rule under Executive Order 14117, effective April 2025 with compliance requirements phasing through October 2025, defines six categories of sensitive personal data and sets volume thresholds for cross-border transfers.

The EU AI Act, in force since August 2024, classifies AI systems by risk tier and requires that training data for high-risk systems be classified, documented, and assessed. The penalties for getting classification wrong are no longer theoretical: Meta's 1.2 billion euro fine in May 2023 highlighted the consequences of inadequate cross-border data transfer safeguards and weak privacy governance. Uber's 290 million euro fine from the Dutch regulator in August 2024 demonstrated how poor data governance and inadequate transfer controls can lead to significant regulatory penalties.



Privacy-by-Design: Embedding Trust into Architecture

If privacy failures originate within architecture and processes, privacy must be embedded within those systems from inception. Privacy-by-Design (PbD), developed by Dr. Ann Cavoukian, provides a proactive framework for integrating privacy into technology, business processes, and organizational culture. Rather than addressing privacy concerns after deployment, PbD seeks to prevent privacy

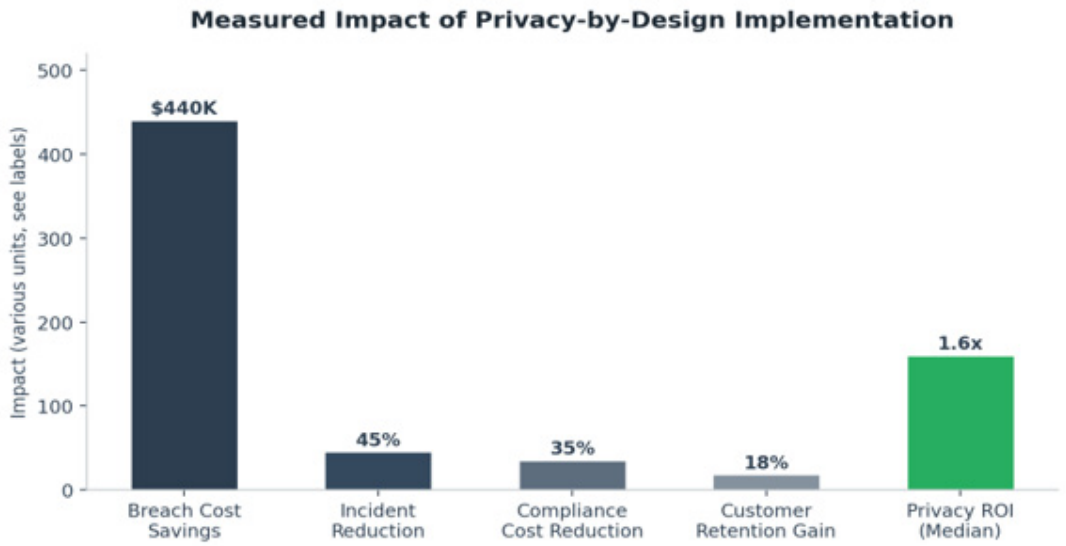
issues before they occur. GDPR Article 25 now mandates data protection by design and by default. Brazil's LGPD Article 46 and India's DPDPA Section 8 impose parallel duties.

Organizations adopting PbD discover that privacy becomes easier and less expensive to manage because controls are integrated into systems from the start. The economic impact is measurable: adding privacy protection after product development costs significantly more than designing it from the beginning. Key implementation practices include data minimization, privacy impact assessments, consent management, transparent data processing, and user-centric privacy controls.

Table 3: Privacy-by-Design Principles and Business Value

Principle	Privacy Outcome	Business Benefit
Proactive, not Reactive	Fewer incidents	Lower remediation costs
Privacy as Default	Automatic protection	Greater customer confidence
Embedded into Design	Reduced privacy debt	Sustainable compliance
Full Functionality	Innovation and privacy coexist	Business growth maintained
End-to-End Security	Lifecycle protection	Reduced breach exposure
Transparency	Accountability demonstrated	Stronger customer trust
Respect for User Privacy	User empowerment	Improved retention rates

Source: Cavoukian (2011), adapted with ISACA DTEF outcomes



Privacy-Enhancing Technologies: Operationalizing Privacy

While Privacy-by-Design provides strategic direction, organizations require technical mechanisms to implement privacy objectives. Privacy-Enhancing Technologies (PETs) fulfill this role by enabling organizations to derive value from data while minimizing privacy risks. Together, PbD and PETs transform privacy from a compliance obligation into a strategic capability.

Privacy-Enhancing Technologies in Practice

Differential Privacy adds calibrated statistical noise to datasets so that individual records cannot be reverse-engineged while aggregate patterns remain accurate. Apple deploys this technique across iOS to collect usage analytics and improve services without ever linking behavioral data to specific user accounts. Google's RAPPOR system applies the same principle to Chrome browser telemetry.

Federated Learning trains AI models across distributed devices or institutional boundaries so that raw data never leaves its source. Instead of centralizing patient records, hospitals participating in a federated network exchange only model updates, preserving confidentiality while still producing clinically useful results. Google adopted federated learning for Gboard keyboard predictions, keeping typing data on-device.

Homomorphic Encryption allows mathematical operations on ciphertext without ever decrypting it. A financial institution can outsource risk calculations to a cloud provider, and the provider returns encrypted results without ever seeing the underlying account data. Microsoft and IBM have published open-source libraries making this technology increasingly practical for production use.

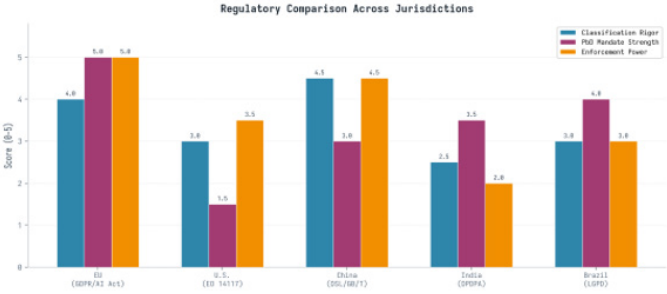
Zero-Knowledge Proofs enable one party to verify a claim without revealing the underlying information. A user can prove they are over eighteen without disclosing their date of birth, or demonstrate sufficient account balance without exposing transaction history. Ethereum-based identity wallets already use this technique for selective credential disclosure.

Governance, Regulation, and Digital Trust

Technology alone cannot restore trust. Sustainable privacy requires governance structures, accountability mechanisms, and regulatory oversight. ISACA's Digital Trust Ecosystem Framework (DTEF), released in 2024, provides a systems-thinking approach across people, process, technology, and organizational dimensions. The World Economic Forum expanded its own trust framework to nine dimensions the same year. These frameworks share a common objective: ensuring organizations manage personal information responsibly and transparently.

Over the past decade, governments worldwide have responded to growing privacy concerns through comprehensive data protection legislation. GDPR mandates Privacy-by-Design and accountability. China's PIPL establishes strict data governance requirements. India's DPDPA introduces Significant Data Fiduciaries subject to stricter obligations. Brazil's LGPD defines sensitive personal data and requires distinct legal bases for processing. ISO 27701:2025, released in October 2025, provides a standalone Privacy Information Management System framework, while NIST's Privacy Framework 1.1 draft, published in April 2025, supports privacy risk management through Identify, Govern, Protect, Communicate, and Monitor functions.

Many organizations continue approaching privacy primarily through regulatory compliance. While compliance remains important, it represents only the minimum acceptable standard. A compliance-focused organization asks: "Are we meeting legal requirements?" A trust-focused organization asks: "Would our customers be comfortable if they fully understood how we were using their information?" Privacy governance should be considered a strategic capability supporting long-term business resilience, aligned with ISACA's DTEF principle that trust is a governance outcome.



Classification Figure 5: Regulatory Comparison Across Jurisdictions — Classification Rigor, PbD Mandate, and Enforcement Power (Sources: GDPR, DOJ, Chinese SAC, Indian MeitY, Brazilian ANPD

The Cost of Negligence: Case Study Insights

Meta: The Compliance Paradox

European regulators imposed penalties exceeding 1.2 billion euros in what remains the largest GDPR enforcement action to date. The Irish Data Protection Commission fined Meta in May 2023 for inadequate data processing safeguards and failure to implement privacy-by-design principles from inception. Beyond the financial penalty, Meta faced significant business consequences: user trust eroded, and regulatory scrutiny intensified across multiple jurisdictions. The case illustrates that compliance alone is insufficient. Transparency and governance matter as much as meeting the letter of the law.

Equifax: When Governance Failures Multiply

The 2017 Equifax breach exposed sensitive information for approximately 147 million individuals. The company subsequently agreed to a settlement of at least $575 million with the U.S. Federal Trade Commission. The incident demonstrated that governance failures magnify technical vulnerabilities and transform security incidents into long-term reputational challenges. Consumer trust recovery took more than three years. Weak governance, inadequate vulnerability management, and poor oversight turned a patchable vulnerability into one of the most damaging breaches in history.

Future Trends: Digital Trust in an AI-Driven World

AI Governance and the Next Trust Challenge

Figure 6: IBM Security. (2025). Cost of Data Breach Report 2025.

Artificial intelligence represents perhaps the most significant privacy governance challenge of the coming decade. Modern AI systems depend upon enormous quantities of information, often sourced from multiple datasets, jurisdictions, and third-party providers. IBM's 2025 research found that 13% of organizations suffered breaches involving AI models or applications; of those, 97% said they lacked proper AI access controls. Organizations must now address questions traditional privacy frameworks were not designed to handle: How is training data collected? Does meaningful consent exist? How is bias identified and mitigated? Can automated decisions be explained? The EU AI Act classifies AI systems by risk tier, requiring documentation of training data quality, bias, and provenance for high-risk systems.

Privacy-Preserving Technologies at Scale

Techniques such as federated learning, synthetic data, and confidential computing will become increasingly important as organizations balance analytical capabilities with privacy protection. The EU AI Act and NIST's draft Privacy Framework 1.1 both point toward PETs as compliance tools for AI governance.

Self-Sovereign Identity

Future identity systems will enable individuals to control credentials and selectively disclose information, fundamentally changing the relationship between individuals and organizations. This aligns with Cavoukian's principle of respecting user privacy and ISACA DTEF's user-centric dimension.

Strategic Recommendations

For Boards of Directors, establishing privacy oversight committees is essential. Organizations with board-level privacy oversight report fewer incidents. Integrating privacy into enterprise risk management, as COBIT 2019 prescribes through APO13 and APO12, ensures that classification and privacy-by-design receive governance attention. Trust metrics should appear alongside traditional KPIs in board presentations.

For CISOs and security leaders, adopting Privacy-by-Design across technology roadmaps reduces remediation costs. Deploying Privacy-Enhancing Technologies where data sensitivity is high, particularly federated learning for AI training and differential privacy for analytics, reduces breach exposure. Maintaining visibility into shadow data repositories is critical: most organizations discover unknown repositories containing significant unaccounted data volumes.

For risk managers, measuring privacy debt as a governance metric provides early warning. Conducting privacy impact assessments before new initiatives, as both GDPR and DPDPA require, prevents privacy debt from accumulating. Privacy risk registers should be aligned with enterprise risk management and re-assessed quarterly.

For product teams, applying data minimization to product design reduces compliance scope and strengthens trust. Enabling privacy by default rather than by choice matters because default settings determine actual behaviour for the vast majority of users. Increasing transparency regarding data processing builds the customer confidence that translates into retention.

Conclusion

The digital economy depends fundamentally on trust. Yet trust cannot be sustained through cybersecurity investments alone. The growing customer trust deficit reflects deeper architectural and governance failures. Excessive data collection, digital profiling, limited transparency, and inadequate user control have weakened confidence in digital systems.

Data classification, Privacy-by-Design, and Privacy-Enhancing Technologies offer a practical pathway toward restoring trust. Classification tells you what you have and what rules apply. Privacy-by-design uses that knowledge to build protections in from the start. PETs make both possible at scale. Together, supported by governance frameworks like ISACA's DTEF and COBIT, NIST's Privacy Framework, and ISO 27701:2025, they create the conditions for measurable digital trust.

The organizations that close these gaps first gain something more durable than regulatory compliance. They keep the 82 percent, the customers who leave after a single privacy failure and who stay when organizations demonstrate accountability. In an era defined by AI and data-driven decision-making, trust is a strategic asset. The organizations most likely to succeed are not necessarily those with the largest datasets, but those that manage data most responsibly.

The Core Pillar: Independence Defines Internal Audit

Independent Audit Creates Organizational Value

Satya Narayan & Laisha Vats
Global Risk Management Institute (GRMI)

Abstract

According to standard definitions internal auditing is independent assurance, each of these terms has a distinct significance. The functions of internal audit have changed tremendously with the development of digital transformation, introduction of artificial intelligence, concerns about cybersecurity and other environmental, regulatory changes creating a dilemma around the tasks and scope of internal audit. Currently, independence should not be perceived simply as conformity to a specific standard, but rather as a vital resource that enables companies to establish their reputation and make decisions based on the objectives mentioned above. The discussion will deal with this issue taking into consideration how we understand the relationship between independence, objective professional judgment and external verification of the results achieved by auditing.

Introduction

The current business environment is characterized by volatility encompassing aspects such as digital transformation, geopolitics, regulatory pressure, and cybersecurity, among other unpredictable factors. While the board of directors and executives need the assurance that the controls are working effectively, they also need independent assurance that would provide them guidance for making viable strategic options. Therefore, the internal audit function has transitioned from being merely a controlling body to being an advisory service provider for the purpose of value addition.

Independence will be explored in this paper to demonstrate that the evolution of the notion of independence has changed the way the meaning of independence should be looked at in this context. It was previously considered to be a professional ability and a requirement of Global Internal Audit Standards,

with all the discussions involving independence referring to the structure of reporting and ethical conduct of internal auditors. Today, independent internal audit can also be defined as independence which provides the ability to challenge internal auditees' recommendations, which is much more than the previous definitions of independence.

Independence Beyond Compliance

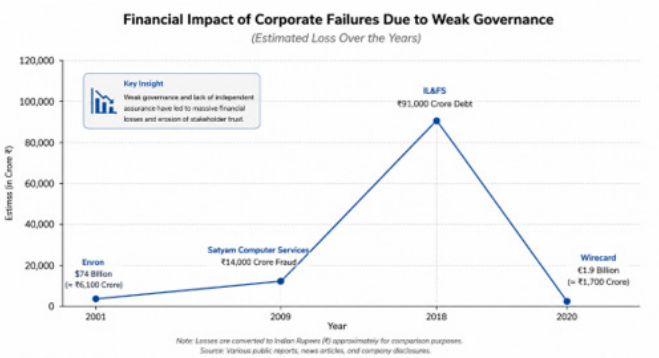
For a long time, independence has been viewed mainly as a form of freedom from management. While the concepts of independence are important as well, independence is something much bigger than that. Independence means the ability to maintain independence in one's judgment and overcoming one's own bias.

Independence will then encompass the organizational dimension and independence as a state of mind. Even reporting directly to an audit committee won't be enough for independence to guarantee reliable audit if auditors don't really challenge management ideas. On the other hand, honest and brave auditors can contribute immensely to corporate governance.

Independence as the Foundation of Organizational Trust

Trust is one of the most important assets for an organization, and internal auditing is one way to ensure that trust is maintained. All parties involved—investors, regulatory bodies, employees, clients, and boards—rely on the fact that they get some assurance from the audits conducted about the governance systems in a given organization, and whether the risks are being managed appropriately. Without the independence that comes with the internal audit, no one is going to believe the audit results, and the confidence of the stakeholders will slowly start to decline.

Internal auditors provide independent evaluations of



the governance affairs of a firm. They achieve this by providing objective and fair assessments about the processes in place in the firm, which do not always have to align with the way that an organization has been doing things up to that point. Hence, the internal audits played by the auditors have always contributed to better governance by forcing organizations to uncover their vulnerabilities early enough before they become serious issue.

Evidence, Objectivity, and Professional,

Skepticism

Independence cannot be achieved without adequate evidence. There should be sufficient confirmation of each audit report. The supportive evidence must be enough to satisfy any professional question concerning its credibility." Since companies increasingly rely on computerized management systems, the reliability of evidence is equally crucial along with the independence of the auditor.

Independence is the connecting factor between the independence and reliability of evidence. General skepticism makes internal auditors challenge all assumptions, check different levels of evidence and note potential discrepancies that may indicate existence of existential risk.

Independence in the Age of Artificial Intelligence and Digital Transformation

The introduction of artificial intelligence, advanced analytics, robotic process automation and continuous auditing has created a huge transformation in the auditing industry. The mentioned technologies help to conduct analysis of data, to find out unusual transactions and to perform audits in a more effective way. One should also remember that technology does not mean independence and professionalism.
Even though AI can be capable to find unusual actions, it does not mean that AI is capable to understand the moral values, mindset and goals of the organization. This means that the limits of things that AI can do are defined by the way it interacts with certain information, i.e. algorithms process information in compliance with certain rules and work with past data which can be erroneous.

Emerging Threats to Auditor Independence

In the present-day climate, influences on independence are not as evidently visible as they used to be. Even when there is an involvement of management in ensuring independence, there are other problems affecting independence such as the use of technological systems and the selection of relevant information from management to undertake decision-making.

Threats to independence should not be seen as taking place at a given time because they are gradual in nature. Their adverse effect on independence manifests itself over time due to the duration of exposure to these threats and the culture of the organization. Therefore, independence is always expected to be guaranteed through adopting and implementing practices that will lead to being independent.

Building Independence into Governance

Instead of being classified as an independent audit requirement, independence must be regarded as part of the organization's governance system. Good governance is based on the existence of a proper internal audit charter, functional reporting lines to the audit committee, access to all relevant information free of charge, and the possibility of comprehensive communication with the board of directors.

It is necessary to take into account independence declaration, conflict of interest assessment, auditor rotation, and continuous professional development of professionals..

Independence as a Strategic Business Advantage

The independent internal audit creates more impact in helping to make decisions than in detecting weaknesses in a control system. This is because the independent internal auditing gives assurance and reduces uncertainty as well as assisting organizations in strategic planning so as to create trust among stakeholders. With the independent internal audit, organizations can react flexibly to various challenges like the new regulations, innovations, disruptive forces, and reputation risks. An internal audit has more responsibilities than just compliance and it provides an independent perspective.

The Future of Independent Internal AI

The increasing degree of interdependence of

Area	Key Performance Indicator (KPI)	Organizational Outcome
Governance	Audit Committee satisfaction	Strong governance culture
Risk Management	High-risk issues identified early	Reduced risk exposure
Audit Quality	Timely implementation of recommendations	Better internal controls
Trust	Stakeholder confidence surveys	Enhanced reputation
Strategy	Audit recommendations adopted	Better business decisions

institutions and technology will keep changing the demands on internal auditors. The future auditor needs to have a technical and analytical ability, ethical sense, and specialized knowledge. Although the technology will continue changing the internal audit processes, independence will be the principal quality of the profession.

and promoting responsible decision making. The continued importance of internal audit shall not depend solely on the capability of adopting relevant technology but also on the principle of independence of the internal audit itself.

Summary

Independence represents much more than one of various things that standards mention. Independence is a principle which brings credibility to the information and gives the assurance its authority and credibility when making decisions by organizations. Nowadays, in this complicated world, rapid digital development takes place

Organizations of tomorrow shall not only vie against one another by innovating but also in the area of trust. Independent internal audit will help in creating that trust through its objective assurance in containing governance issues, fortifying resilience, and stakeholders demand more. Independence enables internal audit to move beyond compliance services. With independence backed by evidence, skepticism, and good governance internal audit values is more than just control of inefficiencies.

Independence: The Soul of Internal Audit

Saba Nawaz & Pravin Khandare
Scholars- Global Risk Management Institute(GRMI)

A synthesized review of theory, technology, practice, and governance auditing, risk management & corporate governance

Abstract

Independence is the foundation of the internal audit profession. In this article, five peer-reviewed articles are used to create a synthesis of the literature on audit theory, risk management, and technology of continuous auditing. In addition, it includes an exploration of the ethical and functional foundations of independence as an important part of effective internal auditing, along with a model that can help ensure that independence is maintained.

Keywords: internal audit independence, corporate governance, risk management, continuous auditing, accountability, agency theory

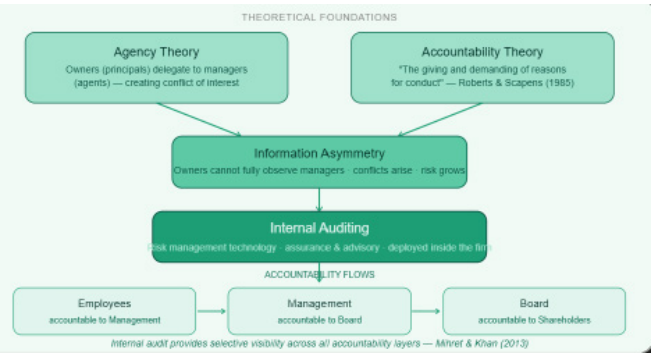
Introduction

Internal auditing is one of the most important facets of effective corporate governance, as it serves as a watchdog, adviser and risk management tool. Internal auditors who lose their independence are simply an official unable to provide any assurance of objectivity.

Five studies provide support for this synthesis: mihret and khan (2013) provide guidance on accountability in theory; farras, ali and audi (2025) discuss the application of ai, rpa and blockchain; njagi (2023) offers guidance and potential threats to independence; and setiawan, rohemah and aulia (2023) raise the question of whether embedded auditors may find there independence. So, therefore we can say that that the independence is significant hence not optional.

Conceptual Framework

The separation of ownership from control creates conflicts between owners and managers (agency theory) that create the need for monitoring. With this as a backdrop, setiawan et al. (2023) says that audit independence decrease agency risk by adding accountability and transparency. However, mihret and khan (2013) argue that accountability through auditor reports is in fact only partially sufficient because they circulate solely within the context of the internal accountability channels established by an organisation, not to the external marketplace. Roberts and scapens definition of accountability as "the giving and approaches of reasons for conduct" gives us a broader perspective by showing a systematic method of selecting the information from employees to boards.

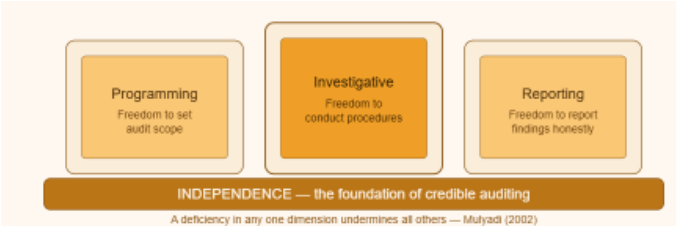


Independence: concept, dimensions, and necessity

Independence means having no prejudice, conflict of interest or undue influence-and thus, being able to make objective judgments on the basis of the facts presented in the audit report. Njagi suggested that independence is the basis of credibility in auditing. Without it, the financial statements are of no use to the users and will erode investor confidence." Mulyadi (2002) as said by setiawan et al. (2023) - describes independence in terms of three dimensions; programming (independently determining audit scope), investigatory (independently performing audit procedures) and reporting (independently reporting results truthfully). Deficiency of some one can also affect other area as well .

Another area of plan is whether internal auditors can be independent because such employees of the organisation being audited. Setiawan et al. (2023) posit that as long as the internal auditor is independent of the department(s) being audited, then independence from the entire organisation can be achieved.

Four additional pillars highlight the independence include: objectivity, reliable audit reports, follow to professional standards (the iia requires independence for all auditors as a precondition for practice), and the prevention of fraud.



Factors threatening independence

A number of factors are included for the issue of independence. The internal auditor has a reporting relationship with the very management that he/she is auditing; nordin (2022) points out that true independence is difficult to achieve when the person under whose leadership you operate is being scrutinized by you. In addition, where the audit function is placed will significantly affect independence in terms of placement under the finance director or the board of commissioners; placement with the former will greatly limit independence, whereas placement with the latter will increase independence. Another source of risk is the capable for being dependent on fees, long-term client safeguarding, having financial interests in the audited entity, and direct management pressure. Moreover, a strong, independent audit committee is largely the means of safeguarding independence.

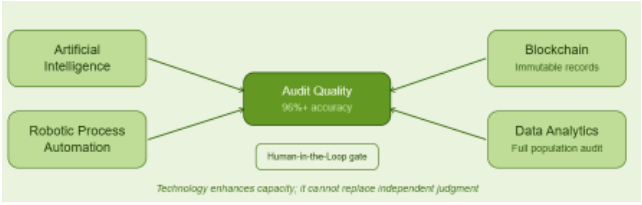
Technology is another risk that has received less attention; as reviewed by farras et al. 2025 have identified that there are points of overlap between continuous auditing systems and performance monitoring for management; thus, where audit technology has integrated with management systems – the distinction between oversight and control is blurred, and the very technology that has been developed to promote quality may serve to undermine independence.

Continuous auditing: technology and independence

As per farras et al continuous auditing includes real-time inspection, controls, and is legally framed

instead of just sampling periodically. High-risk areas are targeted by ai via anomaly detection; rpa minimizes the risk of human error and gives the auditor more time for exercising their discretion; while blockchain gives the auditor a secure audit trail that can't be tampered with.

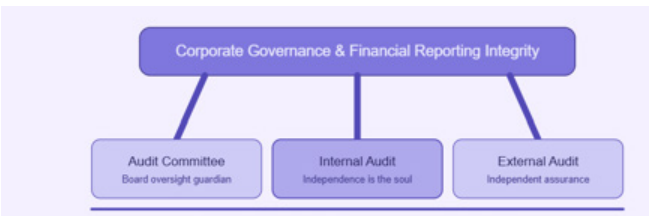
The impact of automation on the accuracy of data is greatest in organizations with high levels of automation; all have achieved at least 96% accuracy; the use of annual training programs and larger sample sizes improved the accuracy of data. While technology can enhance the capacity of an independent auditor, it cannot take the place of independent judgment. Analytical mindset can make bias to the methodology for auditors. Use of a human-in-the-loop framework will assist in ensuring that humans can also make judgments to give output from the machine.



Governance and the audit committee

Internal auditing is a component of the governance model , along with external auditing and the audit committee. This key factor of the following issues includes accuracy of financial reports, investor confidence, compliance, fraud, and stakeholder safeguards.

The audit committee plays a key role among those agencies or individuals responsible for maintaining the independence of the internal auditor. Kamau et al in 2014. As said by njagi , state that the effectiveness of the audit committee is essential in establishing or maintaining this level of independence. Setiawan et al indicate that the chief audit executive needs to have direct access to the board, without any involvement from or interference by management



A framework for sustaining independence

There are four key factors that will enable internal audits to maintain their independence once drawn from all five sources. Such as:

- Structure - internal auditing functions should be functionally reported to the audit committee or the board of directors rather than the executive management of the company, with direct and unfiltered access by the chief audit executive to the chairperson of the board.

- Regulatory and ethical – auditors must adhere to the rules of independence both in fact and in appearance; adhere to the rules for the provision of prohibited services and adhere to the rules for mandatory rotation of auditors. A code of ethics specifically for internal auditors is needed to achieve the standards set out in the current framework of the iia indonesia.

- Technology - continuous auditing systems need to be governed such that the results of ai systems will continue to be evaluated independently through human-in-the-loop review of the ai systems' outputs.

- Culture - professional skepticism is needed and should be cultivated willingly by the board of directors and with continuous education of professionals regarding the competencies required to perform their functions according to an established ethical framework.

Conclusion

The essence of internal auditing is independence. If we are not considering ia then technical structure is left which will be too technical to be used. The content concludes significant conclusion: they represent different perspectives regarding the independent nature of the internal auditor.

Mihret and khan note that the emergence of internal auditing as an it-based risk management tool depends on independent relationships between the internal auditor and the entity being audited for internal auditing to provide value. Farras et al.

Explain that technology can upgrade the quality

of auditing, but it is all about good governance to maintain independence. Setiawan et al. Explain that the independence of an auditor can be viewed from two angles. While the auditor must be independent of the department they work for, they are still performing an audit on behalf of the overall organization as well.

Independence must be proactively established, protected and enhanced in the internal audit profession through structural design, regulatory compliance, technological oversight, and cultural beliefs.

TIME FOR A CROSSWORD

X	S	T	A	F	G	K	K	V	P	P	Z	B	U	E	P	E	U	O	R
K	G	O	Z	Y	N	X	B	Q	G	J	S	X	V	K	R	R	A	G	S
V	O	K	Z	T	Z	L	C	E	N	I	A	K	M	K	S	I	R	U	R
F	V	S	T	I	M	F	T	D	I	Z	C	H	A	R	T	E	R	Y	J
W	E	K	W	R	B	I	N	C	T	P	E	O	T	A	E	R	H	T	H
L	R	O	J	A	Y	G	E	Q	L	J	C	B	F	D	L	Z	B	Y	G
C	N	R	O	I	C	S	C	Q	U	A	N	J	Z	P	Q	E	G	K	P
X	A	O	Q	L	A	D	N	I	S	J	E	E	Y	K	E	Y	D	Q	V
E	N	T	G	I	C	R	A	N	N	X	D	C	B	O	M	M	W	Q	D
G	C	A	A	M	O	A	R	T	O	J	N	T	B	V	T	S	C	K	O
I	E	T	B	A	V	U	U	E	C	D	E	I	Q	Y	V	I	X	J	A
A	S	I	Y	F	D	G	S	G	J	U	P	V	G	K	G	C	G	J	I
S	R	O	S	K	A	E	S	R	Y	O	E	I	V	D	I	I	E	F	I
D	A	N	C	T	R	F	A	I	Q	D	D	T	G	R	L	T	R	K	I
E	W	Z	I	J	S	A	H	T	F	C	N	Y	J	T	K	P	R	O	B
E	A	P	H	V	B	S	D	Y	M	B	I	C	N	M	F	E	W	T	S
U	W	W	T	O	T	D	I	L	I	G	E	N	C	E	L	C	J	K	G
W	Y	V	E	Z	I	M	P	A	I	R	M	E	N	T	R	S	C	Y	Y

HINTS

- Freedom from conditions that threaten unbiased performance of audit duties
- One has to adopt a neutral perspective when dealing with the engagements.
- Measures employed to mitigate risk to independence
- What happens when independence and objectivity can be put at risk
- Advisory engagement whose scope is agreed with the client
- An objective evaluation of evidence to form an independent judgment
- Reassignments of audit personnel, regularly performed in order to reduce risks of familiarity
- The threat that comes about when the auditor advocates for a client's case
- Threat due to long and personal relationship between auditor and auditee.
- Combination of processes by which an organization is directed and controlled
- Code underpinning integrity, objectivity and professional conduct
- Document establishing internal audit's purpose, authority and responsibility
- Global framework that guides the internal audit profession
- Aspect of risk that affects independence
- What internal audit exists, in part, to help manage
- Trait establishing trust and providing the basis for reliance on judgement
- Judgement and thinking abilities should be exhibited in analyzing the evidence presented in documents.
- Every engagement requires having patience and diligence in conducting it.

Please send your answer by email to:
publications@iiaindia.co