www.iiaindia.co

Volume-31 | April 2026 Edition

Internal Audit Today

Magazine of the Institute of Internal Auditors, India

Auditing the New Economy:
Startups, Unicorns & High-Growth Companies

The Institute of Internal Auditors India

Table of CONTENTS

EDITORIAL

EXPERT VOICES - LEADERSHIP SERIES

THE INSIGHT EXCHANGE - AUTHOR'S CANVAS

Table of CONTENTS

WOMEN'S FORUM

EMERGING MINDS – STUDENTS' FORUM

AROUND THE WORLD

IIA INDIA HAPPENINGS

Chairperson's Communique

Navigating the New Economy: The Evolving Role of Internal Audit

Dear Readers,

It gives me immense pleasure to present the latest edition of IA Today, releasing on 1st April, centered on the theme "Auditing the New Economy – Startups, Unicorns, and High-Growth Companies."

We are living in a time where business models are evolving faster than ever before. Startups and high-growth enterprises are redefining industries through innovation, agility, and disruption. While these organizations thrive on speed and scale, they also operate in environments marked by uncertainty, evolving regulations, and dynamic risks. In such a landscape, the role of internal audit is no longer confined to traditional assurance, it is becoming a strategic enabler, helping organizations balance growth with governance.

This edition aims to explore how internal auditors can effectively navigate this new economy. From understanding unconventional business models to evaluating emerging risks in technology, funding structures, and scalability, the insights shared by our contributors reflect the changing expectations from the profession. It is encouraging to see how internal audit is increasingly partnering with management to drive value, strengthen controls, and build sustainable organizations.

I would like to extend my heartfelt gratitude to our dedicated editorial team for their vision, effort, and commitment in curating this insightful edition. My sincere thanks also go to all our esteemed contributors who have generously shared their knowledge, experiences, and perspectives. Your contributions are what make this publication relevant and impactful for our readers.

As we move forward, I encourage each one of you to embrace this shift, continuously upskill, and position internal audit as a forward-looking function that not only safeguards value but also helps create it.

I hope this edition provides you with meaningful insights and practical takeaways as you engage with the evolving business landscape.

Happy Reading!

warm regards,

Pooja Dharewa

Chairperson
IIA India Publication Committee
pooja@kdpractice.com

President Communique

Auditing the New Economy: Sustaining Momentum in Startup Unicorns and High-Growth Companies

Startups, unicorns, and high-growth companies are built on energy. An idea takes hold, momentum builds, and speed becomes the defining advantage. This is how ideas scale rapidly, markets are entered with confidence, and decision-making is often accelerated to match opportunity. In such environments, governance can be perceived as a constraint. In reality, it is governance that enables momentum to be sustained.

For internal auditors, the opportunity is not to slow growth, but to **shape it intelligently, anchored it in sound judgment and structure.**

1. Governance as a Foundation for Sustainable Growth

The early stages of growth are often driven by vision and instinct. As organisations scale, this must be complemented by clarity in roles, accountability, and risk awareness.

Internal auditors bring value by helping leadership pause at critical inflection points to examine whether the organisation's governance framework is keeping pace with its growth. This does not mean imposing rigid structures, but designing mechanisms that are fit for purpose, allowing agility while ensuring informed decision-making.

In such contexts, the advisory dimension of internal audit becomes particularly relevant, enabling the creation of a governance environment that supports both innovation and discipline.

2. Technology, Data, and the AI Landscape

Startup unicorns and high-growth companies are inherently technology-driven. Many rely on data-intensive models and are increasingly integrating AI into core operations.

This introduces new dimensions of risk and assurance.

Internal auditors must extend their lens beyond traditional controls to evaluate the reliability of data, the integrity of algorithms, and the transparency of decision-making frameworks. Weaknesses in foundational elements such as data quality, ownership, and lineage can lead to systemic risks that scale with the business.

The auditor's role, therefore, is to ensure that as organisations adopt advanced technologies, the underlying architecture remains **robust, reliable, and trustworthy.**

3. Strengthening Audit Capability for a Changing Environment

While the operating environment continues to evolve, the fundamentals of internal auditing remain unchanged. Structured thinking, evidence-based evaluation, and professional objectivity continue to form the core of the discipline.

What becomes critical is the ability to apply these fundamentals in new and dynamic contexts.

This requires a commitment to continuous learning, an awareness of emerging business models and technologies, and, importantly, the ability to engage effectively with leadership teams. In high-growth environments, influence is shaped not only by technical expertise, but also by **clarity of communication, contextual understanding, and professional credibility.**

In the new economy, internal audit occupies a pivotal position. It connects ambition with accountability and supports organisations in navigating complexity without losing momentum.

When approached with insight and balance, internal audit does not merely evaluate growth. It helps ensure that growth is **sustainable, resilient, and well-governed.**

With warm regards,

Krishnan Venugopal

President, IIA India

Chief Editor

Dear Esteemed Members and Readers,

Welcome to the April 2026 Edition of Internal Audit Today.
We are living in the age of the new economy—an era where startups, unicorns, and high-growth companies are reshaping industries at breathtaking speed. These organizations thrive on disruption, scale overnight, and attract valuations that redefine possibility. Yet, with rapid ascent comes heightened risk, fragile governance, and the urgent need for assurance that can keep pace.

Auditing the New Economy

In this dynamic landscape, internal audit is no longer a back-office function. It is the compass guiding organizations through volatility, the guardian of trust in markets where confidence is currency. Startups demand agility, unicorns stretch governance frameworks, and high-growth firms test ethical boundaries. The audit profession must rise to meet these challenges—not as a brake on innovation, but as a catalyst for sustainable growth.

From Oversight to Partnership

Traditional checklists cannot capture the complexity of exponential expansion. Auditors must evolve into strategic partners—evaluating governance in venture-backed firms, safeguarding investor confidence in billion-dollar unicorns, and ensuring ethical scaling in companies racing toward global dominance. Technology-enabled assurance, forward-looking risk analysis, and proactive engagement are no longer optional; they are the hallmarks of relevance in the new economy.

The Call to Action

This edition explores practical strategies, case studies, and insights to help auditors embrace this transformation. We highlight how assurance can fuel innovation, strengthen stakeholder trust, and anchor growth in integrity. I invite you to read this issue not just as professionals, but as pioneers. The mission before us is epic: to ensure that the dreams of startups, the ambitions of unicorns, and the momentum of high-growth companies rest on foundations strong enough to endure.

Together, let us champion audit as the invisible engine of sustainable growth and the architect of tomorrow's economy.

Happy Reading!

Jitesh Khushalani

Chief Editor
IIA India Magazine

BEHIND THE SCENES

Pooja Dharewa
Chairperson , IIA India Publication Committee
pooja@kdpractice.com

EDITORIAL & DESIGN TEAM

Jitesh Khushalani
Chief Editor
jiteshk@jkgrcs.com

Arun Kasat
Deputy Editor
kasatarun@gmail.com

Aditya Ghatage
Quality Reviewer
adityaghatage@gmail.com

Chanchal Mishra
Lead Co-ordinator
coordination@iiaindia.co

Sandeep Singh
Design Head
sandeep@letsdigitalmarketing.com

PUBLICATION COMMITTEE

Arjun Golar
Member
arjungolar@gmail.com

Karthik Varadharajan
Member
vksuccess777@outlook.com

Amit Sharma
Member
amitsharma5@hotmail.com

Anand Gupta
Member
anandguptain@gmail.com

Our Contributors

Balkrishna Chaturvedi

This leadership feature traces the professional journey of Balkrishna Chaturvedi, Head of Management Assurance and ESG at Sapphire Foods. The article highlights how curiosity, ownership, and continuous learning shaped his progression from auditing roles to strategic leadership. It underscores the evolving role of internal auditors as business partners who align risk, governance, and operational objectives. The narrative also reflects his leadership philosophy—empowering teams, embracing adaptability, and staying relevant in an increasingly technology-driven environment.

Flip to Page 12

Aditya Kumar S.

Aditya Kumar S. examines the emerging governance challenges created by complex digital ecosystems where enterprises increasingly depend on sub-vendors, cloud infrastructure providers, and embedded technology partners. The article introduces the concept of the "Shadow Supply Chain," referring to hidden layers of technological dependencies that operate beyond direct contractual oversight. By analysing cybersecurity, operational, regulatory, financial reporting, and ESG risks, the article proposes applying frameworks such as COSO to strengthen governance. It also outlines the critical role of internal auditors in enhancing visibility, monitoring vendor ecosystems, and ensuring resilience in technology-driven supply chains. .

Flip to Page 16

Melina Taprantzi

In "Quantifying ESG," Melina explores how organisations can move beyond qualitative sustainability commitments toward measurable and decision-useful ESG performance indicators. The article emphasises the growing expectations from investors, regulators, and stakeholders for credible sustainability data and transparent reporting. It explains how structured metrics, governance frameworks, and integrated reporting practices can help organisations translate ESG initiatives into measurable outcomes aligned with long-term business strategy. The article also highlights the role of internal audit and governance functions in validating ESG data, strengthening reporting integrity, and ensuring accountability in sustainability disclosures.

Flip to Page 27

Abhilash Tewari

In "Cracking the Code of Internal Audit in Modern Finance," Abhilash explores how the role of internal audit is evolving in response to rapid changes in financial systems, regulatory expectations, and technological innovation. The article explains how internal auditors must move beyond traditional compliance-focused reviews to become strategic advisors who provide forward-looking insights on risk, governance, and operational efficiency. By embracing innovation and strengthening analytical capabilities, internal audit functions can enhance organisational resilience and deliver greater value to stakeholders.

Flip to Page 30

Namrata Agarwal

In "IPO Readiness 2.0," Namrata explores how organisations preparing for public listing must move beyond traditional compliance checklists and adopt a more holistic readiness approach. The article highlights the importance of strengthening governance structures, financial reporting frameworks, internal controls, and risk management practices well before entering capital markets. It explains how internal audit can play a critical role in evaluating organisational preparedness, identifying control gaps, and supporting management in building investor confidence.

Flip to Page 34

Prakash Ramaiah

In "Beyond Sampling: The Rise of the Hybrid Auditor," the author examines how the internal audit profession is evolving in response to rapidly advancing technology, data analytics, and complex risk environments. The article highlights the shift from traditional sampling-based audit techniques toward data-driven, technology-enabled assurance approaches. By adopting a hybrid skillset that blends professional judgement with advanced data tools, internal auditors can deliver deeper insights, enhance risk detection, and provide more proactive value to organisations.

Flip to Page 39

Our Contributors


Phani Kiran & Kathiroli B

In "The Hybrid Auditor," the author explores how the internal audit profession is evolving in response to increasing technological complexity and data-driven business environments. The article highlights the need for auditors to develop a hybrid skillset that blends traditional audit expertise with capabilities in data analytics, technology risk, and business strategy. It explains how combining analytical tools with professional judgement enables auditors to move beyond routine compliance checks and deliver deeper insights on emerging risks. By embracing this hybrid approach, internal auditors can enhance organisational resilience and provide more proactive and value-driven assurance.

Flip to Page 42

Ashwin SA

In "The 'Black Box' Challenge," Ashwin, examines the growing difficulty auditors face when evaluating complex systems and technologies whose internal workings are not fully transparent. As organisations increasingly rely on advanced algorithms, automated decision systems, and third-party technology platforms, auditors must assess risks within environments where processes may function as opaque "black boxes." By adopting structured assurance approaches and collaborating closely with technology specialists, internal auditors can better evaluate risks and maintain accountability in increasingly complex digital environments.

Flip to Page 49

Dhiraj Kumar Gupta

In "Continuous Assurance," the author explores how advancements in data analytics and automation are transforming the traditional audit cycle. The article highlights the shift from periodic reviews toward real-time monitoring of controls, transactions, and risk indicators. By leveraging technology-enabled tools and integrated data systems, organisations can identify anomalies earlier, strengthen governance oversight, and respond more proactively to emerging risks. The article also emphasises the role of internal auditors in designing and validating continuous assurance frameworks that enhance transparency, improve control effectiveness, and support more agile risk management practices.

Flip to Page 54

Aayush Bajaj

In "Valuation Scrutiny in Stress Cycles," Aayush examines how periods of market volatility and financial stress place heightened scrutiny on asset valuations and financial reporting assumptions. The article explains how uncertain economic conditions can amplify risks related to fair value measurements, impairment assessments, and management estimates. The article also underscores the role of internal audit in evaluating valuation processes, challenging assumptions, and strengthening oversight to support informed decision-making..

Flip to Page 59

Mallesh Bulusu

The article highlights the shift from task-based automation to agentic AI in internal audit. Unlike traditional tools, agentic AI can independently detect risks, gather evidence, and generate audit findings without human initiation. Auditors then focus on validation and decision-making. While this improves efficiency and insight, challenges like system integration, security, and governance remain. Ultimately, it enhances—not replaces—the auditor's role, emphasizing judgment and strategic risk assessment.

Flip to Page 63

The Institute of Internal Auditors India

EVENT SCHEDULE

APRIL 2026

04 APR

WEBINAR

03:00PM - 05:00PM

AUDIT COMMITTEE EXPECTATIONS FROM INTERNAL AUDIT: DELIVERING INSIGHT, ASSURANCE & VALUE

06 APR

WEBINAR

03:00PM - 05:00PM

AWARENESS SESSION ON CIA CHALLENGE & 3 PART EXAM

11 APR

ANNUAL CONFERENCE

09:00AM - 05:30PM

IIA HYDERABAD AND VIZAG AUDIT CLUB ANNUAL CONFERENCE 2026

18 APR

WEBINAR

03:00PM - 05:00PM

DESIGNING EFFECTIVE AUDIT PROGRAMS: A RISK-FOCUSED AND VALUE-DRIVEN APPROACH

25 APR

WEBINAR

03:00PM - 05:00PM

POWER SKILLS FOR INTERNAL AUDITORS- FROM ASSURANCE TO IMPACT

02 MAY

WEBINAR

03:00PM - 05:00PM

ICOFR

16 MAY

WEBINAR

03:00PM - 05:00PM

WRITING IMPACTFUL INTERNAL AUDIT REPORTS: FROM FINDINGS TO ACTIONABLE INSIGHTS

23 & 30 MAY

WEBINAR

03:00PM - 05:00PM

AI IN IA

WEBINAR

03:00PM - 05:00PM

THE ROLE OF INTERNAL AUDIT IN STRENGTHENING BUSINESS CONTINUITY & RESILIENCE

06 & 27 JUN

WEBINAR

03:00PM - 05:00PM

AUDIT OF NEW-AGE & START UP BUSINESSES

WEBINAR

03:00PM - 05:00PM

AUDITING THE PROCUREMENT & SUPPLY CHAIN FUNCTION

To register for any of these events, please log on to the official website of IIA India at **www.iiaindia.co**

global professional CERTIFICATIONS

SETTING THE BENCHMARK : CIA ACHIEVERS

(Jan-Mar 2026)

Shakti Chauhan
EY

Sahil Shah
Omnicom

Sumana Dongre
Ex - Infosys

Pankaj Kumar
Marelli

Rutba Ayubkhan
EY

Pramod Rao
Wells Fargo

Mohammed Ahasan
HP

Supriya Dhamale
Kotak Mahindra Bank

Niyas TP
Deloitte

Vivek VP
Sundaram Finance

Akshay Bendre
Tecnimont

Aditya Fofliya
Indus Towers

Vikash Chopra
CK Birla Hospitals

Ranjana Ahuja
M/s Aneja Associates

Nupur Arora
Fareportal India

Arun Kumar S
KPMG

Shreya Poojary
Clark Schaefer Hackett

Shyam Sathy
Ford Credit

Vimal Verma
Ahli Bank of Kuwait

Tulsi Khemka
Beyond bookkeeping

Mohammed Shareel
Zand Bank

Santosh Shukla
Ex-Kalpataru Projects International

Rajeeb MTK
Ghassan Aboud Holding

Keerthana Ramachandar
Ex - PKF Sridhar & Santhanam LLP

Ashwin Machado
State Street

Sumit Badale
Commercial Bank International

TALK TO US TODAY

+91 87360 83099

cia@globalprofessionalcertifications.com

JOIN OUR WHATSAPP COMMUNITY

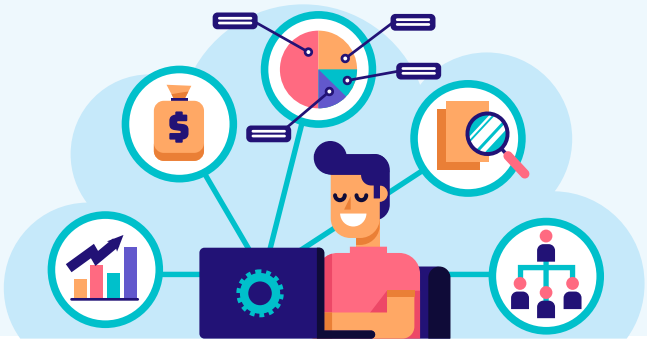
Jeevan Velayudhan
Co-Founder & Director.
MMM Info Solutions Pvt. Ltd

Think Process First. ERP Next. Save Costs Long Term.

Most companies approach ERP systems incorrectly. They assume problems will disappear with new software or an upgrade. That assumption is wrong. The problems already exist in running systems. They show up daily: endless approval delays, inaccurate reports, excessive customizations that add complexity, and processes misaligned with actual work.

The core issues remain constant. Whether planning a new ERP, enhancing an existing one, or optimizing IT overall, you face the same challenges: inefficient processes, layered approvals, fragmented data, and uncontrolled customizations. These do not vanish with new software. They simply transfer to the new platform.

Leading organizations address them first. They stabilize operations before altering the ERP. They deploy targeted Process Micro-Solutions. These fix workflows, cleanse master data, and resolve operational gaps without disrupting the core system.



Why do Process First approach and Micro-Solutions Work?

- Cleans & governs data across ERP & legacy systems.
- Simplifies approvals and operational controls.
- Reduces ERP customization & license dependency.
- Accelerates ERP upgrades and integrations.
- Improves auditability and compliance readiness.
- Enables gradual, low-risk change management.

High-Impact Micro-Solutions provide Quick & Measurable results. Here is how:

- Master Data Cleanup and Governance.
- Approval and Delegation Rationalization.
- Vendor Customer Data Validation.
- Procure-to-Pay and Order-to-Cash Controls.
- Compliance and Document Automation.
- ERP and legacy system integration layers.

These deliver fast execution, low cost, and measurable results often in weeks.

The Results

Stable processes and reliable data provide flexibility. Enhance existing ERP capabilities. Integrate digital innovations. Upgrade or migrate platforms seamlessly Select systems based on business fit, not constraints.

Bottom Line

Fix processes. Clean data. Address issues early. ERP new or current then drives value, not friction.

Author can be contacted at
jeevan@mmminfosolutions.com
for any assistance

EXPERT VOICES LEADERSHIP SERVICES

From Flow to Transformation:

The Evolving Leadership Journey of Balkrishna Chaturvedi

Balkrishna Chaturvedi
Head – Management Assurance and ESG, Sapphire Foods

Some careers are meticulously planned. Others unfold, shaped by curiosity, courage, and the willingness to embrace the unknown. The journey of Balkrishna Chaturvedi, Head of Management Assurance and ESG at Sapphire Foods, is a compelling testament to the latter.

It is a journey defined not by rigid design, but by ownership, adaptability, and an unwavering commitment to growth.

Humble Beginnings, Strong Foundations

Hailing from Mumbai, Balkrishna's foray into the world of finance began along a familiar path, choosing commerce after Class 10 and pursuing Chartered Accountancy.

Yet, beneath this conventional choice lay an unconventional mindset.

Driven by a quiet ambition to continuously evolve, he went beyond the expected—completing Company Secretary (CS) alongside his CA, and later fulfilling a long-cherished goal by pursuing an Executive MBA from Jamnalal Bajaj Institute of Management Studies.

This phase didn't just build academic credentials—it shaped a mindset rooted in discipline, curiosity, and lifelong learning.

The Early Years: Learning Beyond Defined Roles

Beginning his professional journey with Deloitte in 2008, followed by experience at KPMG, Balkrishna gained exposure across industries, functions, and business environments.

But what truly distinguished him was not just the breadth of experience, it was his approach to learning.

He refused to be confined by role descriptions. Instead, he immersed himself in every opportunity, building a strong and versatile foundation that would later enable him to navigate far more complex responsibilities.

The Turning Point: From Auditing to Building

His transition to Sapphire Foods marked a defining chapter.

At a time when the organization was navigating mergers, acquisitions, and rapid expansion, the environment was dynamic and demanding. Where many would see ambiguity, Balkrishna saw possibility.

What followed was not just career progression—it was transformation.

- Led financial audits with consistent, high-quality closures
- Built and standardized cross-functional processes
- Strengthened operational ownership, including receivables and control frameworks
- Played a key role in private equity due diligence and IPO execution
- Established risk management and compliance frameworks
- Spearheaded ESG initiatives contributing to global recognition

What truly differentiated his approach was his problem-solving mindset. Rather than highlighting issues in isolation, he focused on identifying root causes and enabling practical, business-aligned solutions.

He consistently worked towards aligning risk and control objectives with business goals, ensuring that governance frameworks were not seen as roadblocks, but as enablers of sustainable growth.

The underlying theme was clear:

He didn't wait for roles—he created them.

Ownership Over Designation

At the heart of Balkrishna's journey lies a powerful belief:
Ownership drives growth—not titles.

Unrestricted by hierarchy or labels, he focused on what the organization needed rather than what his role demanded.

"Once you take ownership, positions don't matter. The focus shifts to delivering the right outcomes, the right way."

This mindset enabled him to evolve from an internal auditor into a **trusted business partner and strategic contributor.**

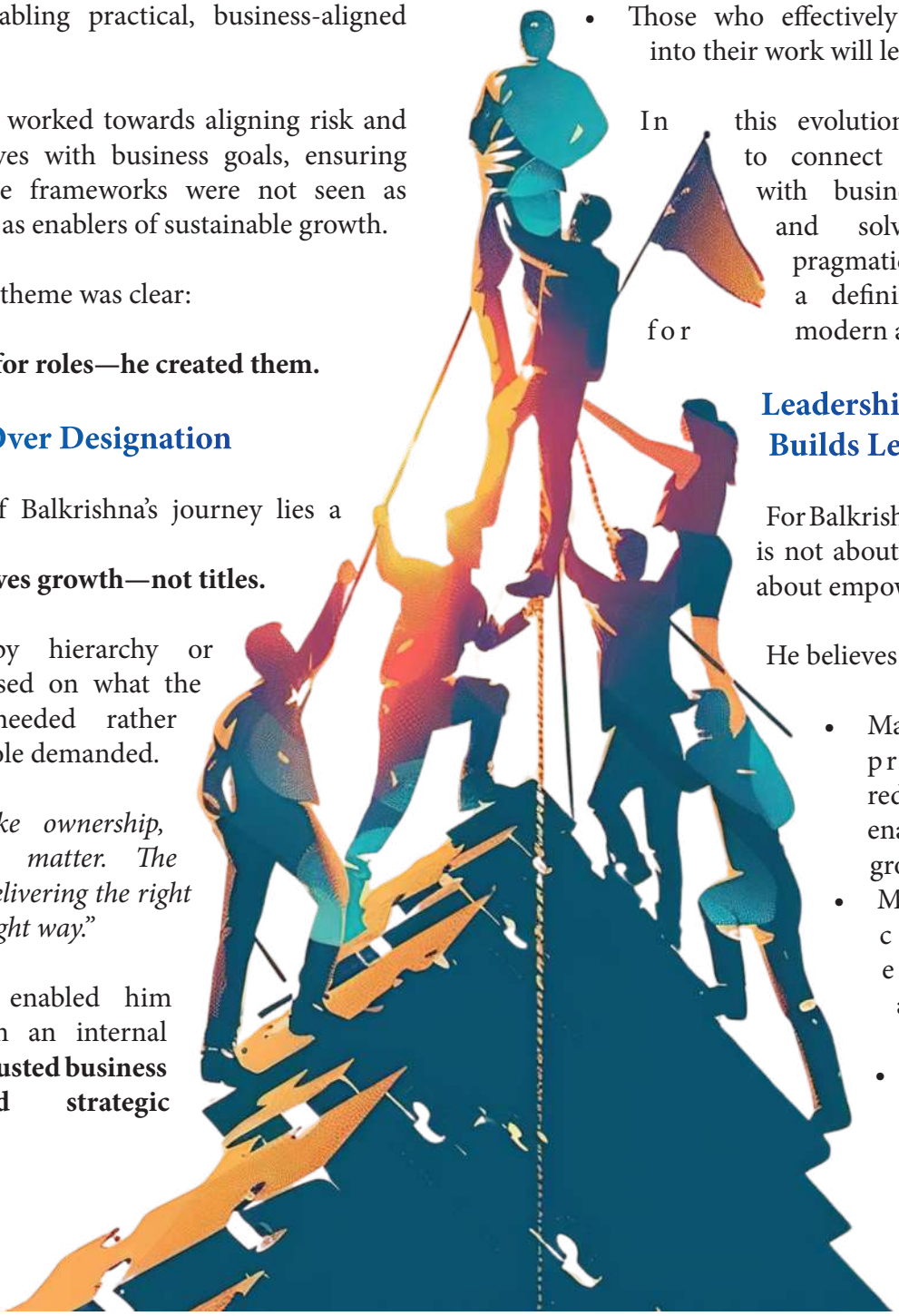
Staying Relevant in a Changing World

In an ever-evolving business landscape, his philosophy is simple yet critical:

Stay relevant. Stay adaptive.
As internal audit continues to transform into a strategic function, Balkrishna emphasizes the importance of deep business understanding, combined with continuous upskilling.

On technology and AI, his perspective is balanced and forward-looking:

- Technology is an enabler, not a replacement
- Human judgment remains irreplaceable
- Those who effectively integrate AI into their work will lead the future



In this evolution, the ability to connect risk insights with business priorities and solve problems pragmatically becomes a defining capability for modern auditors.

Leadership That Builds Leaders

For Balkrishna, leadership is not about control—it is about empowerment.

He believes in:

- Making oneself progressively redundant to enable team growth
- Maintaining consistent engagement and open dialogue
- Offering continuous feedback—not limiting it to annual cycles

- Building a culture of trust and transparency

"When there is trust, solutions emerge. And when solutions emerge, sustainability follows."

His leadership philosophy is grounded in walking alongside the team, not ahead of it.

The Human Side of Leadership

In high-stakes roles requiring tough decisions, Balkrishna brings a deeply human approach.

He recognizes that:

- Authority may deliver short-term compliance
- Trust and empathy drive long-term impact

His approach to conflict is not avoidance, but thoughtful resolution, guided by timing, maturity, and long-term vision.
Sometimes, losing a small battle is necessary to win the larger war.

Beyond Audit: A Purpose-Driven Professional

A qualified Independent Director, Balkrishna's impact extends beyond organizational roles.

He is deeply committed to:

- Strengthening governance practices
- Mentoring and teaching
- Contributing to the professional ecosystem

For him, internal audit is not merely a function, it is a discipline that sharpens business acumen and drives meaningful impact.

The Core Philosophy: Say Yes to Growth

If one idea defines his journey, it is this:

"Say yes to opportunities. That one yes can shape your future in ways you cannot imagine."

Supported by consistency, hard work, and long-term thinking, this philosophy has been central to his evolution.

Key Takeaways from His Journey

- Ownership matters more than designation
- Adaptability is the key to sustained relevance
- Continuous learning is non-negotiable
- Develop a strong problem-solving mindset, not just an observation mindset
- Align risk and control frameworks with business objectives to drive real value
- Leadership is about enabling others to grow
- Trust and transparency build lasting success
- Growth begins the moment you step beyond your comfort zone

The journey of Balkrishna Chaturvedi is not just about professional success, it is about **evolving with purpose, leading with humility, and creating impact beyond defined roles.**

In a world that often emphasizes titles and structured paths, his story is a powerful reminder: **true growth lies in ownership, adaptability, and the courage to keep saying yes to the unknown.**

THE INSIGHT EXCHANGE AUTHOR'S CANVAS

The Shadow Supply Chain

Assessing Sub-Vendor and Third-Party Cloud Risks in the Technology Stack

The post-pandemic acceleration of digital transformation has fundamentally reshaped enterprise operating models. Core business processes now rely on complex technology ecosystems that extend beyond direct vendor relationships, creating new governance and risk management challenges. Business was already focusing on the traditional risks of supply chain and vendor deliverables; the technology related risks appeared, and they continue to hold more importance or attention. Today the risk of technology risk is particularly important since all the resources or activities may not be under our control.

Impact of Digital Transformation on Enterprise Operating Architecture

Digital transformation has fundamentally altered operating architecture. The shift to digital has integrated advanced technology dependencies into core business functions. As organizations increasingly rely on digital solutions, the structure of supply chains has evolved to include a complex web of third-party vendors, sub-vendors, and cloud service providers. This interconnected environment has introduced new challenges, particularly in terms of visibility and control over technology-related risks. Businesses must now address risks not only within direct vendor relationships but also across extended digital ecosystems where sub-vendors and embedded service partners play critical roles. The result is an operating architecture that is more dynamic, yet also more vulnerable to systemic risks and information asymmetries.

Shadow Supply Chain

The Shadow Supply Chain refers to the extended and often opaque digital dependency network comprising third parties, sub-vendors, infrastructure operators, embedded software components, and service partners whose operations materially influence enterprise systems yet remain partially outside direct governance visibility. This construct reflects principal–agent theory challenges and systemic risk characteristics observed in tightly coupled technological ecosystems. Certifications of the processes does not eliminate information asymmetry across multi-tiered vendor chains. Governance must therefore expand beyond direct contractual boundaries to achieve resilience. The technology vendor may not have all the resources to render the service and hence they make use sub-

Aditya Kumar S.
Partner, R.G.N. Price & Co.,
Chartered Accountants

vendors, who is an external entity to deliver part of the service, without a direct contract (no private) with the business. While the business may not select or manage the sub-vendor directly, its systems or operations can still materially affect the business outcomes.

What systems are affected?

Core systems including ERP, treasury platforms, analytics engines, customer relationship systems, and regulatory reporting tools are increasingly deployed in cloud-hosted and outsourced environments. This shift has been driven by scalability, cost efficiency, and innovation advantages. However, governance mechanisms have not evolved at equal velocity. Traditional supply chain oversight was designed for tangible vendor relationships. Modern digital ecosystems are layered, cross-border, API-integrated, and continuously reconfigured.

Risk Categories

The widening gap between operational dependency and governance visibility forms the basis of what may be termed the Shadow Supply Chain. The Risk exposure includes:

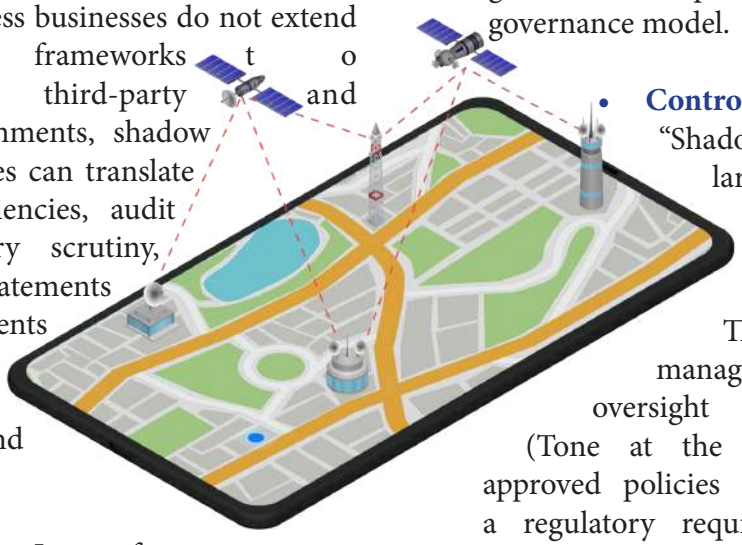
- **Cybersecurity Risks:** Supply chain attacks have proved exploitation of embedded code and credential compromise. In the context of the shadow supply chain, cybersecurity risks arise because businesses increasingly depend on third-party and sub-vendor technologies that operate outside their direct governance and visibility. These dependencies increase the exposure of cyber risks which can result in security failure at any hidden tier of the vendor ecosystem. Cybersecurity Supply Chain Risk Management (C-SCRM) provides comprehensive guidance for managing cybersecurity risks. The standard focuses on risks such as malicious functionality, counterfeit components, poor development practices, and limited visibility into how third-party technologies are designed, integrated, and operated. It outlines expectations at three levels: (a) enterprise level (governance, strategy, and policy (b) business process level (supplier management and criticality assessment (c) system level (system level controls). NIST SP 800 – 161 also deals with supplier and sub-vendor risk management and recommends supplier due diligence, contractual security requirements, monitoring, incident response coordination etc.,

- **Operational Risk:** Concentration risk and cloud region outages can disrupt business continuity. Many businesses rely on cloud service providers to host critical systems and if there is an outage it can have a catastrophic impact on the business. The risk is also amplified because the business

may lack transparency into how their primary vendors further rely on cloud regions or fourth-party providers. The outages can also challenge business continuity and incident response systems and there could be business disruptions.

- **Regulatory Risk:** The Digital Personal Data Protection Act, 2023 imposes accountability on data fiduciaries including sub-contracted entities. Similarly, Reserve Bank of India's – IT Outsourcing and Governing Regulations (RBI Master Direction on Outsourcing of Information Technology Services) requires entities to retain full accountability of outsourced IT services including vendor due diligence, subcontractor visibility, concentration risk management, etc., and also have board-approved outsourcing policies and exit strategies. SEBI's Cyber Security and Cyber Resilience Framework (CSCRF) require entities to assess and manage third-party and vendor risks and be subject to audit. If there are any non-compliances on this front, the penal consequences are heavy, and which would also bring in reputational risk to the business.

- **Financial Reporting Risk:** Section 134(5) of the Companies Act, 2013 requires directors to confirm adequacy of Internal Financial Controls with reference to financial statements. Outsourced systems impacting financial reporting remain within management accountability. Unless businesses do not extend internal control frameworks to explicitly cover third-party and sub-vendor environments, shadow supply chain failures can translate into control deficiencies, audit findings, regulatory scrutiny, and potential misstatements in financial statements resulting in qualifications in audit report and regulatory action.



- **Reputational Risk:** Loss of trust due to service disruption, public perception of poor cyber and technology governance and regulatory actions amplify the reputational damage which could also mean loss of business and how they project themselves in the eyes of their stakeholders.

- **Environmental, Social and Governance Risk :** Where there is a failure of effective oversight of technology and related risks its speaks negatively of 'G' i.e., Governance vertical in ESG, Where customer data is compromised or data privacy has breached and the customer / society feels unsecured the 'S' i.e., Social vertical in ESG is affected and when the vendors depend on inefficient resources, redundant infrastructure and solutions that are not sustainable the 'E' i.e,. Environmental vertical in ESG is affected. These three could pose ESG Risk to the business.

- **Legal Risks:** One of them or all of them or a combination of the risks could pose a serious legal risk to the business including, statutory non-compliances, regulatory enforcement and penalty risks, contractual and indemnity risks, litigation and claims risks, director and management liability risks which needs to be assessed periodically and risk mitigation steps needs to be implemented.

COSO Mapping

This analysis demonstrates how the COSO Internal Control — Integrated Framework can be applied to manage the risks found in "The Shadow Supply Chain." By utilising the five components and seventeen principles of COSO, an organization can bring "shadow" dependencies into a structured governance model.

- **Control Environment:** The "Shadow Supply Chain" exists largely because governance has not evolved at the same velocity as digital transformation. The Board and senior management must expand their oversight beyond direct vendors (Tone at the Top) and have board-approved policies especially where there is a regulatory requirement. COSO provides the framework to institutionalise this. To demonstrate 'commitment to competence,' the organization must recruit or train professionals who understand the complex ecosystems. Management must establish that accountability for a sub-vendor's failure rests with the business, not just the primary vendor.

- **Risk Assessment:** Have risk mitigating measures for the risk arising out of shadow supply chain. Business must assess the likelihood of a sub-vendor outage and the impact on business. The risk assessment must be dynamic to account for continuously evolving technologies and complex supply chain integrations.

- **Control Activities:** Implement automated monitoring and data integrity checks for data flowing from third-party analytics engines. Embed 'right to audit' and 'transparency requirements' into contracts, forcing primary vendors to disclose their own sub-vendor dependencies (the "fourth parties"). To mitigate Operational Risk, control activities should include disaster recovery testing that specifically simulates a failure of a major cloud provider region.

- **Information and Communication:** The shadow supply chain thrives on information asymmetry. Ensure all departments like IT, Legal, Finance, Supply Chain etc., are communicating about sub-vendor dependencies. Develop a communication protocol with vendors that mandates transparency at all levels. If a sub-vendor changes, the business must be notified.

Primary COSO Component	Recommended Action
Control Activities	Implement System-level controls and automated code scanning.
Control Environment	Establish Board-level accountability for data fiduciaries.
Risk Assessment	Map sub-vendor dependencies to specific financial statement assertions
Control Activities	Multi-cloud or multi-region redundancy deployments.
Information & Communication	Obtain sustainability and privacy metrics from the extended value chain.

Responsibilities of Those Charged with Governance:

Designation	Role	Key Accountability Outcome
Chief Executive Officer	Establish Tone at the top integrating digital dependency oversight within strategic governance.	Demonstrate business wide ownership of digital dependency and shadow supply chain risk. There must be periodic Board reporting on technology resilience and critical vendor dependencies.
Chief Financial Officer	Evaluate implications for internal financial controls over financial reporting, assess indemnities, and ensure adequate provisioning and disclosure.	Assurance that all material outsourced and cloud-based systems affecting financial reporting are covered under Internal Financial Controls (IFC), with proper disclosures, provisioning, and risk acceptance documented and approved.
Chief Information Security Officer	Implement structured third-party security assessments, continuous monitoring, and incident response integration.	Assurance that all material outsourced and cloud-based systems affecting financial reporting are covered under Internal Financial Controls (IFC), with proper disclosures, provisioning, and risk acceptance documented and approved.
Chief Information Officer / Chief Technology Officer	Maintain technology dependency inventory and ensure architectural resilience.	A complete, current, and validated inventory of technology dependencies (including fourth parties), with tested architectural resilience and recovery capabilities for critical systems.
Chief Audit Executive	Provide independent assurance over vendor governance effectiveness.	Independent assurance to the Board that shadow supply chain risks are identified, governed, and controlled effectively, including enforceability of contractual safeguards and adequacy of continuous monitoring mechanisms.
Board / Audit Committee	Exercise oversight consistent with COSO ERM governance expectations (RBI Master Direction on IT Governance and Controls (2023) emphasis board-level responsibility for technology risk in regulated entities.	Informed oversight and challenge of management's approach to technology and third-party risk, with documented evidence that accountability for digital and outsourced risks is not delegated but retained at the business level.
Risk Management Committee	The Risk Management Committee should also consider various risks entailing sub-vendor and third-party cloud risks in assessing, monitoring and mitigating activities and provide direction for measures to be taken to ensure there is a robust supervision and oversight.	Integrated assessment and ongoing monitoring of sub-vendor, concentration, regulatory, and systemic technology risks, with clear risk appetite statements and management action tracking for shadow supply chain exposures.

Role of Internal Auditor

Internal Audit must adopt risk-based planning incorporating vendor criticality scoring. Audit programs should evaluate onboarding due diligence, contract safeguards, sub-vendor transparency, and continuous monitoring effectiveness. IT General Controls testing must extend to access management, change management, and incident response coordination across vendor environments.

- **IA Charter:** IA Charter should be amended to explicitly grant the audit function 'right to audit' access through the entire vendor chain, where feasible. IA should have the authority to request SOC 2 Type II reports from critical sub-vendors. Secondly, IA Charter should include digital assets and outsourced cloud environments as audit areas. Thirdly, IA should conduct a 'contractual compliance review' to verify that 'right to audit' clauses are not just present but are legally enforceable down the chain.

- **Bridge between Departments:** The role should act as a bridge between the IT department, procurement, and the Board to ensure a unified view of the shadow supply chain and look at 'concentration risk' of the sub-vendors or vendors relying on the same cloud region. Thirdly, it is crucial to assess how much visibility there is into sub-vendors (fourth parties). High transparency helps maintain oversight and prevent hidden risks from cascading through the supply chain.

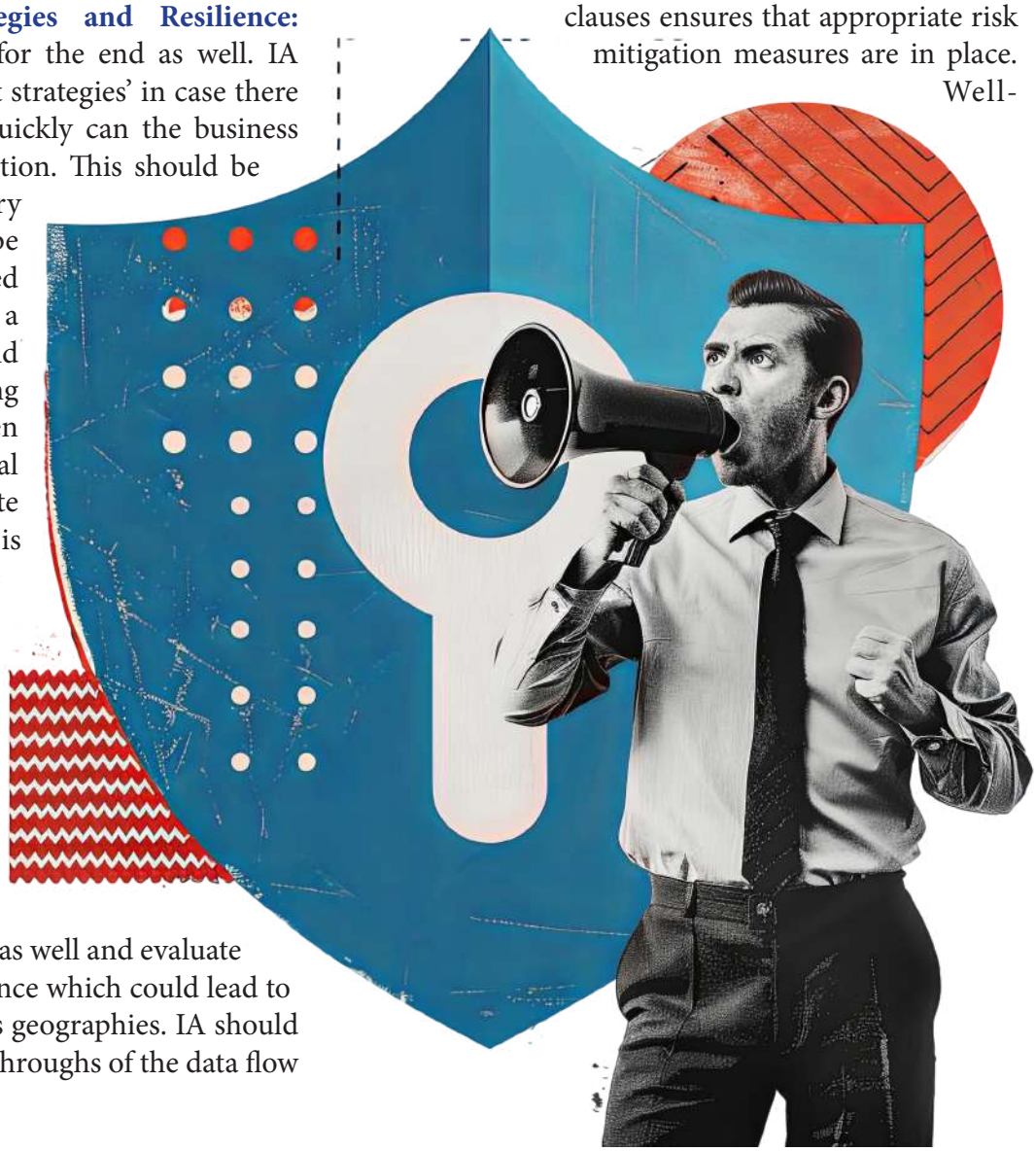
- **Evaluate Exist Strategies and Resilience:** When you plan, plan for the end as well. IA should evaluate the 'exit strategies' in case there are failures and how quickly can the business find an alternative solution. This should be planned and necessary infrastructure must be put in place or notified to be put in place at a short notice. IA should facilitate stress testing that simulate a sudden termination of a critical sub-vendor to evaluate if the exit strategy is operational.

- **Advocacy for 'Privacy by Design':** The Data Protection laws are evolving and different in each geography. IA should ensure that privacy controls are included in the services of sub-vendors as well and evaluate the risk of non-compliance which could lead to penalties etc., in various geographies. IA should perform technical walkthroughs of the data flow across borders to ensure compliance with data localization requirements under the regulation. IA should review data processing agreements to verify that the privacy obligations of the business are mirrored and enforced at every level.

- **Assurance over 'nth party' visibility:** The IA role should evaluate whether the organisation has a registry of even sub-vendors and third-party vendors whose services have materially impact core systems like ERP, Treasury, etc., and audit their relevant controls.

- **Onboarding Due Diligence:** Audits should examine whether vendors are properly vetted before engagement. Effective due diligence minimizes the chances of entering risky or non-compliant relationships. IA should perform testing of recent vendor onboarding to check if the due diligence process included a risk assessment of the vendor's own supply chain.

- **Contract Safeguards:** Reviewing contract clauses ensures that appropriate risk mitigation measures are in place. Well-



drafted contracts, include the 'right to audit,' protect the organization from vendor failures and ensure regulatory compliance.

- **Audit of Shadow Supply Chain Models:** IA must ensure that management understands and monitors that in the new age, 'Shadow Supply Chain' is inherent in cloud services and must ensure that the business first implements its own IT security before relying upon the shadow supply chain. IA should ensure that the relevant data is secured and has enough access control and data encryption to prevent it from being compromised.

- **Real-time and Continuous Monitoring:** Periodic audit is thing of the past in today's scenario given that digital ecosystems are continuously evolving and reconfigured. IA can leverage technology to monitor sub-vendor performance metrics in real-time. IA can establish automated alerts that trigger an audit inquiry whenever a sub-vendor's performance or security score drops below a per-defined threshold or there are other red flags raised.

- **Upskilling and Talent Management:** Along with the IA Team, even the Board and respective committee members should be aware of emerging risks. IA may involve hiring IT specialists who understand the complexities and other professionals like legal experts to have their advice on the contracts, right to audit and other complexities. IA should develop a competency matrix for the audit team that includes cybersecurity certifications ensuring that the function has the 'commitment to competence.'

- **Internal Financial Control Oversight**: IA should map critical financial assertions to specific cloud-hosted modules and verify that the controls identified in the vendor's SOC reports are implemented and tested by the business.

Conclusion

The Shadow Supply Chain is an inevitable outcome of digital interdependence. Regulatory expectations in India and internationally reinforce that accountability cannot be outsourced. Resilient businesses will integrate digital supply chain governance within Enterprise Risk Management, strengthen contractual safeguards, deploy continuous monitoring tools, and empower Internal Audit with technological capability. Digital resilience is determined not by ownership of infrastructure, but by disciplined governance of dependencies. The role of internal auditor is to this as more of an opportunity, rather than a challenge.

IIA India Bombay Chapter

Internal Audit Functional Track Series 16th Jan – 20 February

The Institute of Internal Auditors (IIA) Bombay Chapter successfully conducted its Internal Audit Functional Track Series from 16 January to 20 February 2026, with sessions held every Friday.

This comprehensive learning series was designed to strengthen both functional and behavioral competencies of internal audit professionals. It covered critical business cycles such as Procure-to-Pay, Order-to-Cash, Hire-to-Retire, and Expense Management, providing participants with practical insights into risk areas, controls, and audit approaches. In addition, dedicated sessions on Report Writing, Communication, and Soft Skills helped enhance the effectiveness of auditors in conveying insights and driving value within organizations.
The program witnessed an excellent response, with approximately 323 participants actively engaging across sessions. The interactive format, combined with expert-led discussions and real-world examples, ensured a rich learning experience for attendees from diverse industries.

Overall, the series received highly positive feedback, with participants appreciating the relevance of topics, quality of content, and practical applicability. The initiative reflects the IIA Bombay Chapter's continued commitment to building strong internal audit capabilities and fostering professional excellence within the audit community.

Masterclass Series on AI – 17th Jan to 21 Feb 2026

The IIA Bombay Chapter recently hosted an engaging Masterclass Series on AI, featuring Mr. Saumajit Bandopadhyay. The sessions covered Fundamentals of AI, Responsible AI, and AI Regulations, held on Saturday from 11 AM to 1 PM. Around 175 participants attended, actively engaging in discussions and interactive case studies. Feedback was overwhelmingly positive, highlighting the session's relevance and quality. The Masterclass provided a platform to explore AI opportunities and responsibilities, reinforcing IIA Bombay Chapter's commitment to knowledge sharing and professional development. Overall, the event was a resounding success.

Knowledge Sharing Session - Internal Audit Report Writing and Communication to Stakeholders, 14th Feb 2026

The IIA Bombay Chapter hosted a focused knowledge-sharing session on Internal Audit Report Writing and Communication to Stakeholders on 14th February from 11 AM to 1 PM. The paid session, attended by 21 participants, provided practical guidance on effective report drafting and stakeholder communication, enhancing internal audit impact.

21 Feb 2026 - Cyber Risk Assurance Beyond ITGC

The Bombay Chapter successfully conducted a webinar on "Cyber Risk Assurance Beyond ITGC" on 21st February 2026 from 3:00 PM to 5:00 PM. The session was delivered by Mr. Nimit Shah, who shared valuable insights on evolving cyber risk landscapes and the need to go beyond traditional IT General Controls (ITGC) in ensuring robust assurance frameworks.

The webinar received an encouraging response, with a total of 314 registrations and 284 participants attending the session. The audience actively engaged throughout the discussion, reflecting strong interest in the topic. The overall feedback rating for the session was 3.52, indicating a positive reception and scope for further enhancement in future sessions. The Bombay Chapter continues to take such initiatives to promote knowledge sharing and professional development among members.

28th Feb 2026 - Integrating ESG Risks Into the Internal Audit Plan: A Practical Framework

The Institute of Internal Auditors Bombay Chapter conducted a webinar on "Integrating ESG Risks Into the Internal Audit Plan: A Practical Framework" on 28th February, led by Shailesh Haribhakti.

The session saw an excellent response with 359 registrations and around 297 participants attending. The speaker highlighted the growing importance of integrating Environmental, Social, and Governance (ESG) risks into internal audit processes and shared practical insights on building a structured audit approach aligned with organizational goals.

The webinar was well received, with participants appreciating the relevance, clarity, and actionable takeaways, making it a valuable learning experience for internal audit professionals.

7 march 2026 - Strengthening Governance through Effective IFC Audit

The Institute of Internal Auditors Bombay Chapter successfully hosted a webinar on "Strengthening Governance through Effective IFC Audit" on March 20, 2026, from 3:00 PM to 5:00 PM. The session was led by renowned speaker Gaurav Agarwal, who shared valuable insights on enhancing governance frameworks through robust Internal Financial Controls (IFC) audits.

The webinar witnessed an encouraging response, with 271 registrations and around 239 active participants. Attendees gained practical perspectives on strengthening internal controls, improving risk management, and ensuring compliance through effective audit practices.

The session was highly engaging and well-received, reflecting the growing interest in governance and audit excellence among professionals.

7th March IIA Bombay Chapter Women's Day celebration
The Balanced Woman: Nutrition, Movement & Mental Wellness.

The Bombay Chapter of the Institute of Internal Auditors hosted a special Women's Day celebration on 7th March 2026, centered around the theme "The Balanced Woman: Nutrition, Movement & Mental Wellness." The in-person session brought together around 15 participants for a meaningful and engaging experience focused on holistic well-being.

The event featured a blend of insightful discussions, breathwork, interactive activities, and a calming sound bath session, all facilitated by wellness coach Venu Aadhya Hirani. Participants appreciated the opportunity to pause from their busy professional lives, connect with like-minded women, and focus on self-care in a supportive environment.

The session received very positive feedback, with attendees leaving feeling refreshed, centered, and empowered. Overall, the event was a successful initiative by the Bombay Chapter to celebrate Women's Day with purpose and impact.

14th March - Leveraging Artificial Intelligence in Internal Audit Practices

The IIA Bombay Chapter successfully hosted a webinar on "Leveraging Artificial Intelligence in Internal Audit Practices" on 14th March. The session, delivered by Rajiv Gupta, received an encouraging response with 379 registrations and over 320 active participants.

The webinar provided valuable insights into the role of AI in enhancing audit efficiency, accuracy, and risk assessment. It was well-received by attendees, as reflected in the positive feedback, making it a highly engaging and insightful learning experience

Quantifying ESG

Moving beyond marketing to audit the carbon footprint of AI and data centers

Artificial intelligence has quickly become the defining technology of our time. It is transforming the way businesses operate, how decisions are made, and even how knowledge itself is created and distributed. From financial forecasting to healthcare diagnostics, AI promises speed, insight, and efficiency on a scale we have never experienced before.

Artificial intelligence is often presented as a clean technology. It helps companies optimize supply chains, reduce energy waste, improve climate forecasting, and accelerate scientific discovery. In sustainability discussions, AI is frequently framed as part of the solution.

Yet behind every AI system lies a vast and energy-intensive infrastructure.

AI models run in data centers filled with servers and specialized chips that operate continuously. Training advanced models can require thousands of processors working simultaneously for weeks. Cooling these machines requires water and electricity. Manufacturing the hardware involves energy-intensive supply chains and rare materials. In other words, intelligence at scale has a physical footprint.

As organizations rapidly integrate AI into operations, ESG leaders are beginning to confront an uncomfortable reality: while companies measure emissions from travel, buildings, and logistics, the environmental impact of their digital infrastructure often remains largely invisible.

This is where ESG must move beyond storytelling and into measurement. The real question is no longer whether AI can support sustainability. The question is whether organizations are measuring the sustainability of AI itself. And that begins with auditing its footprint.

Mapping the footprint

The first step in auditing the environmental impact of AI is understanding where computation actually happens. Many companies rely on a mix of internal servers and cloud providers, often spread across different regions. Sustainability teams need visibility into where AI models are trained, where they are deployed, and how frequently they run. Without mapping these activities, it is almost impossible to estimate their environmental impact.

Melina Taprantzi
Founder of the Consulting
Company Earth and Co

Once this digital map exists, organizations can begin measuring energy consumption. Most cloud platforms now provide tools that estimate emissions associated with computing workloads. Platforms from Google Cloud, Microsoft, and Amazon Web Services offer dashboards that translate cloud usage into carbon estimates based on the energy mix of the data centers involved. These tools provide an initial baseline, allowing companies to understand how much carbon is associated with their AI operations.

But auditing AI goes deeper than simply reviewing cloud dashboards. A meaningful audit also examines the lifecycle of AI models. Training models typically consumes far more energy than running them in production. Organizations should therefore track how frequently models are trained or retrained, how long training processes run, and how much computing power they require. Surprisingly, many teams retrain models more often than necessary, creating unnecessary energy consumption.

Another critical part of the audit focuses on model efficiency. Larger models are not always better models. In many cases, optimized or smaller models can deliver similar results with significantly lower computational demand. Evaluating model size, architecture, and performance relative to energy consumption allows companies to identify opportunities to reduce emissions without sacrificing functionality.

Infrastructure choices also matter. The same AI workload can have very different environmental impacts depending on where it runs. Data centers powered by renewable energy produce far fewer emissions than those relying on fossil fuels. As part of an audit, organizations should examine the geographic location of their computing resources and the carbon intensity of the electricity powering them.

Utilization rates provide another important insight. Many servers run at partial capacity, consuming energy even when not performing meaningful work. Improving workload scheduling, consolidating computing resources, and eliminating idle capacity can significantly reduce unnecessary energy use.

An often overlooked dimension of AI audits involves hardware itself. High-performance chips and GPUs have significant embodied carbon due to complex manufacturing processes. Organizations should assess how frequently hardware is replaced, how equipment is recycled, and whether longer life cycles could reduce environmental impact.

What makes auditing AI particularly challenging is that the relevant data is often scattered across departments. Sustainability teams may track emissions, but IT departments manage infrastructure, while data science teams control model development. A credible AI footprint

assessment therefore requires collaboration across these functions.

This cross-functional approach is increasingly becoming part of what some experts call Green AI—the idea that energy efficiency should become a design principle for artificial intelligence systems. The companies that lead in this area are beginning to integrate environmental metrics directly into AI development. Engineers track energy consumption alongside model accuracy. Large training jobs are scheduled when renewable electricity is available. Infrastructure decisions are made with both performance and sustainability in mind.

For ESG leaders, this represents a new frontier. Digital infrastructure is no longer invisible. It is rapidly becoming one of the fastest-growing sources of energy demand in the modern economy.

Auditing the carbon footprint of AI does not require perfect data from the beginning. What matters is starting the process: mapping digital operations, measuring compute usage, evaluating model efficiency, and understanding the energy sources behind data centers.

Once organizations begin measuring these impacts, they can start managing them.

And in the era of artificial intelligence, that may become one of the most important steps toward truly sustainable innovation.

IIA India Hyderabad Chapter

"The President of IIA India, Krishnan Venugopal, along with Madhuri Krishnaswamy(President, IIA Hyderabad Chapter) and Mukundan K V KV (CEO, IIA India), were invited to address the State Bank of India Internal Audit Conclave held in Hyderabad on 14th–15th March 2026.

The sessions covered two critical themes shaping the future of the profession:

- Internal Audit: Current Landscape — including emerging developments, the role of AI, and the evolving vision of internal audit
- Global Internal Audit Standards (GIAS) — certification process and implementation roadmap for SBI

While internal auditors are often invited to business forums, what stood out in this conclave was the unprecedented presence of SBI's top leadership, including:

Chairman Challa Sreenivasulu Setty

Managing Directors Ashwini Tewari, rana ashutosh kumar singh, Rama Mohan Rao Amara, Ravi Ranjan
Deputy Managing Director & CAE Rajeev K. along with other senior leaders.

The presence of the entire leadership team strongly underscores the strategic importance of the Internal Audit function as a key pillar of corporate governance. Such visible commitment from the top sets a powerful benchmark for institutions across both public and private sectors.

Special appreciation to the leadership of Ravi Ranjan (Managing Director) and Rajeev K. (Deputy Managing Director & CAE) for driving this initiative. We are also pleased to note the participation of George Kalliath and Venkata Chaitanya, FCA, CISA, CFE, PGDCLCF (Sr. VP & BOG Member, IIA Hyderabad Chapter, respectively) in the panel discussions, contributing valuable perspectives.

Our best wishes to the Internal Audit team at State Bank of India for continuing to uphold the highest standards of governance. IIA India remains committed to supporting such impactful initiatives that strengthen the profession."

Cracking the Code of Internal Audit in Modern Finance

The rise of New Age Finance Companies commonly known as FINTECH has reshaped the financial services industry. With the introduction of innovative digital products that not only enable faster transaction but also enhance the overall customer experience. The Fintech firms have changed how the Financial Services are delivered. These companies heavily rely upon new age technologies such as Blockchain, Cloud computing, data analytics and Artificial Intelligence to provide their customers services efficiently and effectively as against the traditional financial institutions.

Though this technology driven model bring with them several advantages but also create new and complex risks along with multiple operational challenges. As a result the role of Internal Audit in these fintech organizations becomes more demanding and far different than those in conventional financial institutions. In order to conduct effective Internal Audits in fintech companies the auditors must adopt new approaches and develop specialized technological skills and use flexible audit methodologies that can keep up with the rapidly evolving technological environment.

In this article below we highlight few challenges and strategies to overcome them for performing an effective Internal Audit.

Unique Nature of Operations

One of the primary challenges in conducting internal audits in fintech companies is the technology-driven nature of their operations. Unlike traditional financial institutions where the reliance is on well-established processes and legacy systems, fintechs operate with rapidly evolving platforms, APIs, and digital infrastructure. Core processes such as lending, credit, payments, onboarding, and fraud detection are automated and integrated with multiple third-party systems. For internal auditors, this creates difficulty in understanding complex technological architectures and identifying control points. Traditional audit techniques that focus primarily on manual processes or financial documentation may not be sufficient to evaluate automated systems. Auditors must assess system configurations, algorithms, and data flows, which require a strong understanding of information technology.

Strategy to Overcome:

Organizations should promote collaboration between internal audit teams and IT specialists. Internal auditors should also develop competencies

Abhilash Tewari
Shriram Finance Ltd
Head Internal Audit

in IT auditing, cybersecurity, and data analytics. Continuous training programs and certifications in technology risk management can significantly enhance the effectiveness of fintech internal audits.

Rapidly Changing Regulatory Environment

Fintech companies often operate in regulatory grey areas or under evolving regulatory frameworks. Regulators across the world, including central banks and financial authorities, are continuously issuing new guidelines for digital lending, payments, data protection, and customer due diligence.

For internal auditors, keeping track of these regulatory changes and ensuring that fintech operations remain compliant can be challenging. Unlike traditional financial institutions where regulatory frameworks are relatively stable, fintech regulations may change frequently to address emerging risks.

Strategy to Overcome:

Internal audit teams should adopt a proactive regulatory monitoring approach. Establishing a regulatory watch mechanism, maintaining close coordination with compliance teams, and integrating regulatory updates into audit planning can help auditors remain aligned with the latest requirements. Periodic compliance audits and thematic reviews focusing on new regulations can also ensure timely identification of gaps.

Dependence on Third-Party Service Providers

FinTech's often rely extensively on third-party vendors for critical services such as cloud hosting, payment gateways, KYC verification, data storage, and fraud detection. While outsourcing enables fintechs to scale quickly and reduce infrastructure costs, it also introduces significant operational and security risks.

For internal auditors, assessing risks related to third-party vendors can be complex. Auditors may have limited visibility into the internal control environment of external service providers. Additionally, fintech firms may integrate multiple vendors within their technology ecosystem, increasing the complexity of vendor risk management.

Strategy to Overcome:

Internal auditors should emphasize Third Party risk management frameworks. This includes reviewing

due diligence procedures, service level agreements (SLAs), data security protocols, and periodic performance evaluations either remotely or preferable onsite. Organizations should also obtain independent assurance reports such as SOC reports from critical vendors to strengthen oversight.

Cybersecurity and Data Privacy Risks

Fintech companies handle vast amounts of sensitive financial and personal data. As digital platforms become more widespread, the risk of cyberattacks, data breaches, and identity theft increases significantly. Internal auditors must evaluate the effectiveness of cybersecurity controls, encryption mechanisms, authentication protocols, and incident response frameworks.

However, cybersecurity threats evolve rapidly, and attackers continuously develop new techniques to exploit vulnerabilities. Internal auditors may find it difficult to keep pace with the dynamic nature of cyber risks.

Strategy to Overcome:

Internal audit teams should incorporate cybersecurity assessments into their annual audit plans. Conducting regular IT security audits, vulnerability assessments, and penetration testing can help identify weaknesses in the organization's digital infrastructure. Internal auditors should also work closely with information security teams to understand emerging cyber threats and evaluate the effectiveness of preventive controls.

Data Integrity and Algorithmic Risks

Many of these New age finance companies rely heavily on advanced analytics, machine learning algorithms, and automated decision-making systems. For example, digital lenders may use algorithms to determine creditworthiness based on alternative data sources such as transaction history, social data, or behavioral analytics.

From an internal audit perspective, verifying the accuracy and fairness of such algorithms presents a significant challenge. Auditors must ensure that the data used in these models is reliable, unbiased, and appropriately governed. Additionally, algorithmic errors or biases may lead to incorrect decisions, regulatory scrutiny, or reputational damage.

Strategy to Overcome:

Internal auditors should implement model risk management reviews. This includes validating data sources, reviewing algorithm development processes, and assessing the governance mechanisms around automated decision-making systems. Independent validation of models and periodic performance monitoring can ensure reliability and transparency. Additionally the Internal Auditors must test each of the rule engine independently to ensure that the outcomes are as per the defined model.

Scalability and Rapid Business Expansion

Fintech companies often experience rapid growth as they scale their digital platforms and customer bases. While this expansion drives innovation and market penetration, it may also result in operational controls lagging behind business growth. Processes that were initially designed for small-scale operations may become inadequate when transaction volumes increase significantly.

Internal auditors may face challenges in evaluating whether internal controls remain effective during periods of rapid expansion. Additionally, fintech startups may prioritize speed and innovation over control frameworks, creating potential governance gaps.

Strategy to Overcome:

Internal audit functions should adopt a risk-based audit approach that prioritizes high-impact areas such as customer onboarding, transaction monitoring, fraud prevention, and regulatory compliance. Continuous auditing techniques using data analytics can also help monitor high-volume transactions in real time.

Limited Audit Maturity in Startups

Many fintech companies begin as startups with lean organizational structures. In the early stages, internal audit functions may not be fully established, and formal control frameworks may be limited. This can create challenges in implementing structured audit processes and maintaining independence of the audit function.

Internal auditors may also encounter resistance from business teams that perceive audit activities as slowing down innovation.

Strategy to Overcome:

Building a strong governance culture is essential. Senior management and the board should recognize internal audit as a strategic partner rather than merely a compliance function. Establishing clear audit charters, reporting lines to the audit committee, and promoting awareness of risk management can strengthen the credibility and effectiveness of the internal audit function.

Conclusion

Fintech companies operate in a dynamic and technology-driven environment characterized by rapid innovation, evolving regulations, and complex digital ecosystems. These factors create significant challenges for internal auditors tasked with evaluating risk management, internal controls, and regulatory compliance.

To effectively address these challenges, internal audit functions must evolve alongside the fintech industry. Developing technological expertise, adopting risk-based audit methodologies, strengthening vendor oversight, and integrating cybersecurity assessments into audit programs are essential strategies. Furthermore, fostering collaboration between audit, compliance, IT, and business teams can enhance the overall governance framework.

By embracing these strategies, internal auditors can provide meaningful assurance and advisory support to fintech organizations, helping them manage emerging risks while continuing to innovate and grow in an increasingly competitive financial landscape.

IPO Readiness 2.0

Navigating Heightened Governance Standards for the 2026 Unicorn Class

Over the past decade, global capital markets have witnessed a surge in companies transitioning from venture-backed private enterprises to publicly listed corporations. Over the same period, however, the regulatory and governance expectations surrounding initial public offerings (IPOs) have evolved significantly.

The IPO journey now demands far more than financial performance and market traction. Regulators, institutional investors, and public market stakeholders expect robust governance frameworks, mature internal controls, transparent disclosures, and demonstrable risk oversight before companies access public capital.

Companies aspiring to list in global markets must therefore institutionalise governance structures and operational discipline comparable to those of established public companies. For the 2026 cohort of unicorns and high-growth enterprises, the IPO journey therefore requires a conscious transformation from founder-centric decision-making models to institutional governance and accountability.

The new governance bar for IPO-bound Unicorns

Historically, many high-growth companies prioritized scaling revenues and customer acquisition while deferring governance structures until just before listing. Recent regulatory developments and high-profile governance failures have led to a much higher bar for IPO preparedness.

A few illustrative developments:

India: The SEBI (Listing Obligations and Disclosure Requirements) Regulations (LODR) have expanded requirements on board governance, related party transaction oversight, and disclosure obligations for listed companies.

United Kingdom: The UK Corporate Governance Code 2024 applies from January 1, 2025, with Provision 29 requiring a board declaration on the effectiveness of material internal controls from January 1, 2026.

Middle East: Several jurisdictions have recently enhanced corporate governance requirements for listed companies and companies in the process of listing, with greater emphasis on board effectiveness, internal controls, and disclosure.

Namrata Agarwal

Governance leader, Risk & Compliance (GRC), Internal Audit, and ICoFR/IFC advisory

The OECD Principles of Corporate Governance underscore that strong board oversight and accountability mechanisms are critical for protecting shareholder interests and maintaining market confidence.

Alongside regulators, institutional investors now scrutinise board effectiveness, diversity, independence, and risk oversight when evaluating IPO candidates. For prospective issuers, "good enough for listing" has effectively been replaced by "credible under public scrutiny from day one."

Translating "Navigation" into an IPO Governance Roadmap

In the context of IPO Readiness 2.0, "navigating" heightened governance standards means moving from reactive compliance to a deliberate, sequenced governance build-out.

In practical terms, management should not wait until the DRHP/RHP stage to "fix" governance. The smarter approach is to run a structured readiness programme 18–24 months ahead of listing, built around five integrated governance workstreams that together form the IPO governance roadmap.

First, establish the right board architecture: The foundation of IPO governance is a board that can genuinely challenge, guide, and oversee management. This means refreshing composition early, adding genuinely independent directors, and constituting audit, nomination, remuneration, and risk committees with clear charters and reporting lines.

Governance failures in the IPO process often begin with weak board challenge rather than weak paperwork. WeWork remains the classic cautionary example: its 2019 S-1 highlighted concentrated founder voting power, and the company withdrew its IPO weeks later as investor confidence deteriorated.

The lesson for the 2026 unicorn class is clear: board architecture and independence are not cosmetic; they are price-of-entry issues.

Second, treat internal controls as a pre-IPO value lever: Internal controls can no longer be approached as a last-mile listing formality. They are increasingly a valuation and credibility lever. Companies should document key processes, map risk and control matrices, test design and operating effectiveness, close ITGC gaps, and define management certification protocols.

Arm Holdings is a useful example: in its 2023 F-1, it disclosed a material weakness in IT general controls and laid out a remediation plan involving

access controls, change management, monitoring, external experts, and audit committee oversight; in its amended filing, it stated there were no material weaknesses.

That is what credible navigation looks like: identify, remediate, evidence, disclose.

Third, upgrade financial reporting discipline: IPO-bound companies must demonstrate that their numbers are not only accurate but also produced, challenged, and communicated in a disciplined way. IPO-bound companies need a faster close, technically robust accounting papers, disclosure committees, and consistency between board decks, prospectus language, and investor messaging. This is especially important in areas like revenue recognition, share-based payments, related-party arrangements, and non-GAAP or alternate performance measures.

The burden is no longer merely to "have numbers" but to show that finance, legal, secretarial, and business functions are aligned behind the same disclosure narrative.

Fourth, formalise risk governance: Risk management must move from an implicit management activity to a visible, structured board-level function.

Tata Technologies is a useful Indian example. its annual report states that, as part of the listing process and in line with SEBI LODR requirements, it constituted a Risk Management Committee, and its internal audit framework was positioned to meet internal governance standards and comply with the Companies Act and SEBI LODR.

For 2026 issuers, the message is clear: exchanges and investors increasingly expect formal risk governance, not informal, management-only risk discussions. A well-defined risk appetite, a risk register, and regular risk reporting at board and committee level are rapidly becoming standard.

Fifth, hardwire governance over assurance providers: The governance ecosystem around IPO candidates now extends well beyond statutory audit. One underappreciated change in India is the sharpened governance around secretarial audit. SEBI's 2024–25 changes introduced eligibility,

tenure and prohibited-services guardrails: an individual secretarial auditor may be appointed for one five-year term, a firm for up to two five-year terms, and certain conflicting services are prohibited. Fresh appointment mechanics also apply from FY 2025–26.

For IPO candidates, this effectively means that the entire ecosystem of statutory auditors, secretarial auditors, internal auditors, and other advisors must be structured to ensure independence, rotation, and clear reporting lines well before filing. Boards and audit committees will be expected to demonstrate that they actively oversee this assurance landscape.

The implication for the 2026 unicorn class

The real question is no longer, "Are we ready to file?" It is, "Can we withstand public-market scrutiny on governance from day one?" For the 2026 unicorn class, the winners will be those that treat IPO readiness as an enterprise transformation program; with board refresh, controls remediation, assurance independence, risk governance, and sustainability reporting all managed through a single leadership agenda.

In this environment, governance is no longer the last chapter of the IPO story. It is one of the first things investors read.

IIA India Delhi Branch
Momentum. Innovation. Influence

The first quarter of 2026 set the stage for a powerful start at IIA India – Delhi Branch. With dynamic discussions, forward-looking themes and strong industry participation, our committees came together to create platforms that didn't just share knowledge—but sparked transformation across the internal audit profession.

Training Committee: Future-Ready Learning

- The Training Committee delivered a power-packed webinar on "AI & Generative AI in Internal Audit", attracting 165+ professionals. The session, led by Anand Prakash Jangid, offered practical insights into AI's growing role in auditing.
- A roundtable with EY on "AI Governance & Risk Management" brought together 40+ senior leaders, fostering rich, experience-driven discussions on emerging priorities.
- The committee continues its focus on fundamentals with an upcoming session on "Basic Internal Audit Procedures & Techniques".

Student Development Committee: Building Tomorrow's Professionals

In collaboration with Raffles University, Neemrana, a seminar on "Bridging Academia & Industry – Vision 2030" engaged 150+ students and professionals. Key discussions covered Cyber Risk, DPDP Act, New Labour Codes and the CIA pathway, reinforcing the importance of aligning academic learning with industry expectations.

PSU Forum & Conference Committee: PSU Summit 2.0

The flagship PSU Summit 2.0, held on 25th February 2026, brought together 150+ participants and 20+ speakers under the theme "Reinventing Governance, Assurance & Risk in a Digital-First Public Sector."

Graced by distinguished leaders including Gyaneshwar Kumar Singh, Saurav Mitra and Rajnesh Singh, the summit featured engaging panel discussions on:

- Internal Audit as a strategic partner
- Vigilance & fraud risk in a digital era
- Technology, data analytics & AI in assurance

Supported by leading organizations such as Powergrid, GAIL, ONGC, NBCC, Oil India Ltd. and Trilegal, the event also included motivational and spiritual sessions, making it a holistic experience.

Women's Forum: Expanding Perspectives

The Women's Forum led impactful conversations through insightful sessions:

- "Care Economy as a Governance Issue" by Harsha Ramnani, highlighting ESG audit gaps
- A fireside chat on "Behind GDP Numbers" by Smriti G. Bhatia, emphasizing the invisible economic contributions of women
- "Navigating Corporate Pressure", with 120+ participants, where Shankar Ghosh Choudhury shared practical leadership insights

The forum also contributed a thought-provoking blog:
"Why the Care Economy Belongs in the 'G' of ESG."

Publication & Research Committee: Thought Leadership in Action

- Internal Audit Priorities for 2026
- Objectivity in Internal Auditing
- Using AI in Internal Audits – Opportunities & Challenges

Additionally, insights from the Fraud Survey (Fraud 360°) were released, highlighting emerging fraud trends and risks.

With every initiative, every conversation and every connection, IIA India – Delhi Branch continues to move one step closer to its vision—
to inspire, to lead and to transform the future of internal auditing.

Beyond Sampling: The Rise of the Hybrid Auditor

Bridging the Talent Gap by Integrating Data Science into Internal Audit

When the Data Tells a Different Story

During a routine portfolio review in one of the financial institution, an internal audit team noticed an unusual trend. A cluster of loans had been approved within minutes of application submission. On the surface, everything appeared compliant - documentation was complete, credit scores were acceptable, and underwriting approvals were properly recorded.

Yet when auditors examined the broader dataset, the pattern became more intriguing. Many of the applications shared similar borrower profiles, closely timed approvals, and recurring device identifiers used during submission. When the entire loan population was analysed using data analytics rather than traditional sample testing, the analysis revealed potential weaknesses in parts of the underwriting workflow.

What initially appeared compliant revealed deeper concerns when viewed through data patterns rather than documentation alone.

This scenario reflects a growing reality across industries, particularly in NBFCs and digital lending ecosystems, where operational decisions are increasingly driven by automated systems and vast volumes of data. In such environments, traditional audit techniques may struggle to keep pace with the scale and complexity of transactions. This raises an important question for the profession: How can internal audit provide meaningful assurance in organizations where risk increasingly resides within data?

The answer may lie in the emergence of the **Hybrid Auditor.**

A New Risk Landscape

Over the past decade, expectations from internal audit have expanded significantly. Boards and audit committees now expect assurance not only on compliance but also on emerging risks linked to technology and digital operations.

Internal audit functions are increasingly asked to assess areas such as:

Prakash Ramaiah
IIA Bangalore Treasurer

- digital lending platforms and automated underwriting
- data integrity across interconnected systems
- fraud patterns embedded within transaction datasets
- algorithm-driven decision-making processes
- cybersecurity and technology governance risks

At the same time, the scale of operations has grown dramatically. Financial institutions process thousands—or even millions—of transactions every day. In such environments, relying solely on sample-based testing may limit the ability to detect hidden risk patterns.

Compounding this challenge is a persistent talent gap in internal audit, particularly in areas such as data analytics, automation, and digital risk. While auditors possess strong expertise in governance and controls, many teams lack the analytical capabilities required to examine complex datasets effectively.

Enter the Hybrid Auditor

The future of internal audit does not lie in replacing auditors with technologists, nor in expecting every auditor to become a data scientist. Instead, the profession is evolving toward integrated audit teams that combine complementary skills.

This is the foundation of the Hybrid Auditor model. In this approach:

- Auditors bring domain expertise, control knowledge, and professional scepticism.
- Data scientists contribute analytical techniques, statistical modelling, and automation capabilities.

Together, these capabilities allow internal audit to move beyond traditional control verification toward deeper insights into operational behaviour and emerging risks.

Rather than relying solely on sample testing, hybrid audit teams can analyse entire populations of transactions, identify anomalies, and detect potential control breakdowns earlier. The result is a more insight-driven and forward-looking audit function.

Why Data Science Matters in Internal Audit

Integrating data scientists into audit teams can significantly enhance assurance in data-rich environments.

From Sampling to Full-Population Analysis

Traditional audit relies heavily on sampling techniques. Data analytics enables auditors to examine complete datasets, improving coverage and reducing the likelihood of overlooking hidden anomalies.

Identifying Hidden Patterns

Advanced analytics can uncover patterns that manual reviews might miss, such as unusual approval trends, repeated policy overrides, abnormal borrower clusters, or suspicious transaction timing.
Continuous Auditing

Automated data pipelines and analytics tools enable internal audit to shift from periodic reviews toward continuous monitoring of risk indicators.

Strengthening Fraud Detection

Data scientists can build models that identify behavioural anomalies and unusual transaction flows, strengthening fraud risk monitoring.

Collaboration: The Real Game Changer

The real value of the hybrid model lies in collaboration between auditors and data specialists.

Auditors frame the key governance questions:

- What behaviour's indicate potential control breakdowns?
- Where might policy overrides occur?
- What anomalies might signal fraud?

Data scientists then translate these questions into analytical models that examine large datasets.

The outcome is a powerful combination of human judgment and analytical insight, enabling internal audit to identify risks more effectively.

The Hybrid Audit Model

The Hybrid Audit Model integrates audit expertise with analytics capabilities through a structured approach:

This model combines audit judgment, analytics capability, and governance insight to deliver stronger assurance.

The Future of Internal Audit

The internal audit profession stands at an important point of transformation. As organizations become increasingly digital, automated, and data-driven, the nature of risk itself is evolving.

Providing assurance now requires more than reviewing policies or testing small samples of transactions. It requires the ability to analyse patterns, interrogate data, and understand complex systems.

The Hybrid Auditor represents the profession's response to this shift—bringing together governance expertise and analytical capability to deliver deeper and more relevant assurance.

For audit leaders, the question is no longer whether analytics and data science should be integrated into internal audit. That transformation is already underway.

The real challenge is how quickly audit functions can build teams capable of combining audit judgment with data intelligence.

Takeaway

"In a world where risk increasingly hides within data, the auditor of the future will not just test controls—they will interrogate data, challenge algorithms, and translate complexity into governance insight."

The Hybrid Auditor

Bridging the Talent Gap by Integrating Data Scientists into Internal Audit Teams

Internal audit functions today operate in an environment defined by rapid technological change, increasing data volumes, and evolving risk landscapes. Boards and senior management no longer expect internal audit to merely confirm compliance with policies and controls. Instead, they increasingly expect audit teams to deliver deeper insights, anticipate emerging risks, and contribute to strategic decision-making.

The traditional model of internal auditing—largely centered on financial controls, checklists, and compliance testing—is therefore undergoing a significant transformation. While these methods remain important, they are increasingly insufficient in an era characterized by big data, digital platforms, and complex technology ecosystems.

This shift is redefining the skills required within internal audit teams and creating a growing need for **hybrid talent that combines audit expertise with advanced analytical capabilities.**

The Emerging Talent Challenge

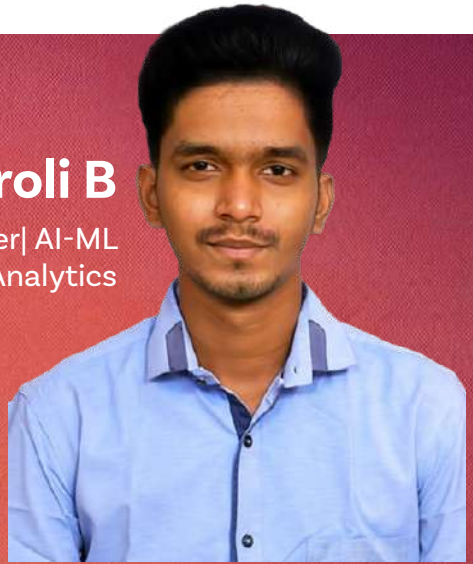
Chief Audit Executives (CAEs) across industries are encountering difficulty in attracting and retaining professionals who possess both traditional audit competencies and advanced technological skills. The challenge is not simply a shortage of auditors; rather, it is a widening gap between the skills traditionally associated with the profession and those required in today's data-driven business environment.

Modern auditors are expected to interpret large datasets, evaluate technology-enabled processes, and identify risks embedded within complex digital systems. However, many internal audit functions continue to rely primarily on professionals with backgrounds in finance or accounting, with limited exposure to advanced analytics.

A survey conducted by Gartner involving Chief Audit Executives in 2025 highlighted that technology adoption and data analytics are among the top strategic priorities for internal audit functions in the coming years.

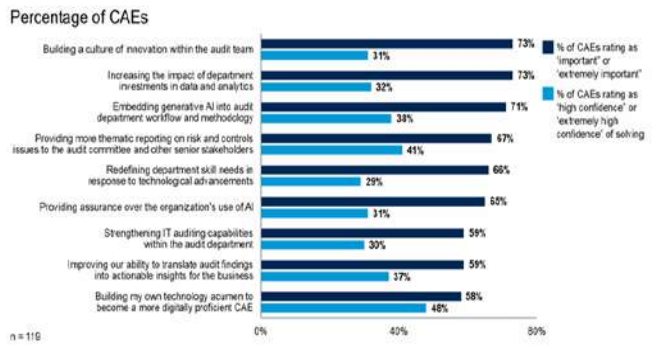
Technology is increasingly seen as a key enabler for expanding audit coverage, improving efficiency, and delivering more meaningful insights to stakeholders. However, realizing these benefits requires internal audit teams to rethink their talent strategies.

Phani Kiran
Head - Internal Audit
MRF Limited



Kathiroli B
Full Stack Developer| AI-ML Developer|Data Analytics

The TOP CAE Priorities for 2026 and confidence in addressing them:



Source: Gartner Survey Shows Audit Departments Are Embracing AI and Data Analytics to Drive Innovation in 2026

The Role of Data Science in Internal Audit

Data science has emerged as a powerful capability and helpful in achieving Internal audit function's objectives.

Following are key differentiators Data Scientists bring to the Internal Audit domain:

- Data science techniques such as statistical modelling, anomaly detection, and automated data analysis using tools like Python-based data pipelines, Pandas for data manipulation, and NumPy for numerical computation
- Advanced audit analytics also leverages machine learning algorithms for pattern recognition, enabling early identification of fraudulent transactions and control weaknesses.
- Statistical techniques such as regression analysis, clustering algorithms, and time-series analysis to identify unusual patterns in transactional data. These techniques allow auditors to detect anomalies, identify control breakdowns, and uncover hidden relationships within complex datasets.
- Usage of specialized data analytics tools such as IDEA (Interactive Data Extraction and Analysis) /ACL enables full-population testing, exception reporting, and automated audit procedures, significantly enhancing audit efficiency and accuracy.

This transition of Data Science being part of Internal Audit function's capability, enables a shift from traditional sampling to full-population data analysis, supported by automated scripts, rule-based validations, and anomaly detection models.

To achieve this transformation, many organizations are beginning to incorporate **data scientists and analytics specialists into their internal audit teams.**

Technical Capabilities

A modern hybrid auditor is expected to have working knowledge in:

- Data extraction and transformation (ETL processes) from ERP systems such as SAP or Oracle
- Querying large datasets using SQL
- Scripting and automation using Python
- Data manipulation using libraries such as Pandas and NumPy
- Data visualization and dashboard development using tools such as Microsoft Power BI or Tableau
- Audit analytics using tools like IDEA and ACL.
- Application of statistical techniques such as regression analysis and clustering
- Working with structured, semi-structured, and unstructured datasets

Integrating Data Scientists into Internal Audit

Successfully integrating data scientists into internal audit functions requires thoughtful planning across several dimensions.

A) Rethinking Hiring Practices

Traditional audit hiring models typically focus on roles such as audit executives or senior auditors. However, as analytics becomes more central to audit activities, organizations should consider capability-based hiring strategies.

Recruiting professionals with backgrounds in data science, statistics, or data analytics can significantly enhance the analytical capabilities of the audit function. These individuals bring expertise in programming, statistical analysis, and data visualization, enabling audit teams to uncover patterns and insights that may otherwise remain hidden.

B) Positioning Data Scientists within Audit Teams

Within internal audit functions, data scientists often operate as internal analytics specialists supporting multiple audit engagements.

Initially, their role may involve developing dashboards or producing analytical reports. Over time, however, their contribution becomes more strategic as they design automated analytics models that help auditors identify anomalies, assess risk patterns, and analyze large volumes of data efficiently.

By enabling data-driven auditing, data scientists help internal auditors expand their coverage and focus on higher-risk areas rather than relying solely on manual verification.

C) Structuring Analytics Capabilities

Organizations typically adopt one of three models when integrating data scientists into internal audit functions:

Decentralized Model:
Data scientists are embedded within specific audit teams and support audits related to particular business functions.

Centralized Model:
A dedicated analytics team provides data science support to multiple audit teams.

Hybrid Model:
A combination of both approaches, where data scientists support individual audit engagements while also contributing to a centralized analytics center of excellence.

In practice, the hybrid model often proves most effective because it balances specialized support with the benefits of shared knowledge and standardized analytics tools.

D) Collaboration and Data Access

Unlike operational departments, internal audit functions typically do not own the underlying data required for analytics. Instead, data must be obtained from various business functions, and definitions or structures may evolve as processes change.

Consequently, data scientists within internal audit must collaborate closely with business process owners, IT teams, and data management specialists. Such collaboration ensures that analytical models are built on reliable and relevant data sources.

In many organizations, early analytics initiatives within internal audit also act as catalysts for broader digital transformation efforts by highlighting opportunities for improved data governance and accessibility.

E) Upskilling the Audit Workforce

While hiring data scientists is an important step, it should not replace efforts to develop analytical capabilities among existing auditors.

Organizations should invest in training programs that help auditors build foundational skills in analytics and technology. Examples include training in programming languages such as Python and SQL, as well as data visualization platforms such as Microsoft Power BI and Tableau.

Mentorship programs, cross-functional collaboration, and micro-learning initiatives can further help auditors gradually develop the skills needed to operate effectively in a data-driven environment.
Ultimately, the goal is to develop hybrid auditors—professionals who combine deep business understanding with analytical expertise.

Practical Applications of Data Science in Internal Audit

The value of integrating data science into internal audit becomes particularly evident when examining common audit processes. Some of such scenarios are elaborated below:

HR and Payroll Audits

Scenario: In large manufacturing environments, payroll costs often depend on employee attendance

and shift participation. Internal auditors must ensure that payroll payments are accurate, complete, and supported by valid attendance records.
Challenge: In a factory employing approximately 2,000 workers across multiple shifts, attendance records can easily exceed several hundred thousand entries annually. Traditional audit approaches typically rely on reviewing a limited sample of records due to the difficulty of analyzing such large datasets manually.

Solution: Data Scientists addresses this challenge by integrating data analytics, attendance records, shift schedules, payroll calculations, and employee master data into a centralized analytics platform. Automated validation rules and anomaly detection techniques can then identify inconsistencies such as payroll payments without corresponding attendance records, abnormal attendance patterns, or discrepancies between attendance logs and payroll calculations. The results enable the Internal Audit team to focus on high-risk cases rather than relying solely on limited sample-based verification.

Accounts Payable Audits

Scenario: Accounts payable processes involve processing a high volume of vendor invoices related to raw materials, services, and capital expenditures. Internal audit teams must ensure that invoices are valid, supported by purchase orders and goods receipt confirmations, and not paid more than once.
Challenge: Traditional audit methods typically examine only a small sample of invoices, leaving the majority of transactions unreviewed.

Solution: Data analytics allows auditors to evaluate the entire population of invoices by integrating accounts payable data with purchase order and vendor master records. Automated analytics can identify duplicate invoices, invoices without supporting documentation, price discrepancies between purchase orders and invoices, and payments made outside agreed contractual terms. The audit team members can make focussed audit efforts on these identified high-risk items rather than relying on limited sample-based testing.

Procurement Audits

Scenario: Procurement functions in manufacturing organizations generate thousands of purchase orders annually. Internal auditors must ensure that purchases are supported by approved requisitions, aligned with operational needs, and executed at competitive prices.

Challenge: In a traditional audit environment, auditors rely largely on their experience and business understanding to select a limited sample of purchase transactions for detailed verification. This involves manual examination of individual purchase orders and related supporting documents, which is time-consuming and resource-intensive. Given the high volume of procurement transactions, such a sampling-based approach may not provide comprehensive coverage or sufficient assurance that procurement activities.

Solution: The data scientist integrates data relating to procurement, inventory, and vendor datasets and applies rule-based analytics and anomaly detection models to automatically identify exceptions such as purchase orders raised without approved purchase requisitions, purchases made despite sufficient inventory and abnormal price deviations compared to historical or competitive vendor prices. The results are presented through dashboards in tools like Microsoft Power BI, enabling the Internal Audit team to continuously monitor procurement practices, detect risks across the entire population of transactions, and provide stronger assurance on compliance with internal procurement controls.

Conclusion

Internal audit functions must evolve to remain relevant in an increasingly digital and data-intensive environment. Integrating data scientists into audit teams represents a powerful strategy for expanding analytical capabilities and improving audit effectiveness.

By combining traditional audit expertise with advanced analytics and investing in the development of hybrid talent, organizations can significantly enhance their ability to detect risks, analyze complex datasets, deliver meaningful insights to stakeholders and help organizations in improving control environment, eliminate/early detect fraud risks/ potential frauds.

The emergence of the Hybrid Auditor—professionals who bridge the gap between auditing and data science—will play a critical role in shaping the future of the internal audit profession.

IIA India Bangalore Chapter

11/02/2026- CAE Roundtable Conference

The IIA India Bangalore Chapter hosted a successful roundtable discussion on February 11, 2026, at the Renaissance Bengaluru Race-Course Hotel, sponsored by Protiviti, bringing together 36 participants including CROs, CAEs, speakers, and members of the Board of Governors. The in-person event, held from 5:30 PM to 7:30 PM followed by cocktails and dinner, provided a vibrant platform for industry leaders to exchange insights on emerging challenges in risk management and internal audit, foster collaboration between CROs and CAEs, and strengthen professional networks, making it a memorable evening of knowledge-sharing and fellowship.

12/02/2026 & 13/02/2026- National Conference

The Institute of Internal Auditors India, together with the IIA India Bangalore Chapter, proudly hosted the IIA India National Conference 2026 on February 12–13, 2026 at the historic Taj West End, Bengaluru. With 544 participants including internal auditors, CAEs, risk leaders, CXOs, consultants, and innovators, the two-day event centered on the theme "The Auditor's Ascent: Scaling New Heights", celebrating the evolving journey of auditors as drivers of competence, courage, clarity, and continual elevation. Through immersive sessions on scalable digital governance, enterprise leadership, purpose-driven governance, resilient leadership, and technical excellence, attendees gained deep insights from visionaries and industry leaders, experienced transformative storytelling, and explored cutting-edge capabilities in AI, analytics, and emerging technologies. The conference fostered reflection on professional growth, strengthened peer connections, and reinforced the vital role of auditors in elevating organizations, industries, and society.

20/03/2026- PDM- DPDP Act

The IIA India Bangalore Chapter held a Professional Development Meeting (PDM) on March 20, 2026, at the Radisson, Bengaluru, with 61 participants in attendance. The session, titled "DPDP Act, 2023 and DPDP Rules, 2025 – An Internal Auditor Lens," explored India's transition into a formal data protection regime and provided auditors with practical insights into the framework's requirements. Discussions focused on how organizations must reassess the collection, use, storage, and sharing of personal data across customers, employees, and vendors, while equipping internal auditors with immediate priorities to strengthen governance, compliance, and assurance in this evolving regulatory landscape.

21/03/2026- Prompt Engineering Session

On March 21, 2026, the IIA India Bangalore Chapter celebrated International Women's Day with a special full-day session on Prompt Engineering at Miles Education, Koramangala, attended by 20 participants. The program equipped auditors, finance professionals, consultants, and students with practical skills to communicate effectively with AI systems, covering fundamentals of prompt design, structuring techniques, business use cases in audit, finance, reporting, and analytics, as well as methods to improve accuracy and reduce hallucinations. Through hands-on exercises, real-time demonstrations, and discussions on ethical and responsible AI use, the session provided actionable insights that participants could immediately apply in their professional roles, making it a highly interactive and impactful learning experience.

The “Black Box” Challenge

Auditing Explainability and Data Integrity in AI-Native Startups

Artificial Intelligence has rapidly become the backbone of many modern startups. In many of these companies, AI is not just a supporting technology, it is the product itself. From automated credit scoring and fraud detection to hiring recommendations and healthcare diagnostics, AI systems are making decisions that directly impact people and businesses.

However, behind the impressive capabilities of AI lies a growing concern often referred to as the “Black Box” problem.

In the AI world, a black box describes a system where we can clearly observe the inputs and outputs, but the internal decision-making process remains opaque. Even developers and organizations that build these models sometimes struggle to explain precisely how the system arrived at a particular conclusion.

For auditors, regulators, and stakeholders, this raises an important question:

If we cannot explain how AI makes decisions, how can we trust those decisions?

This is where two fundamental principles become critical: Explainability and Data Integrity.

Understanding Explainability in AI

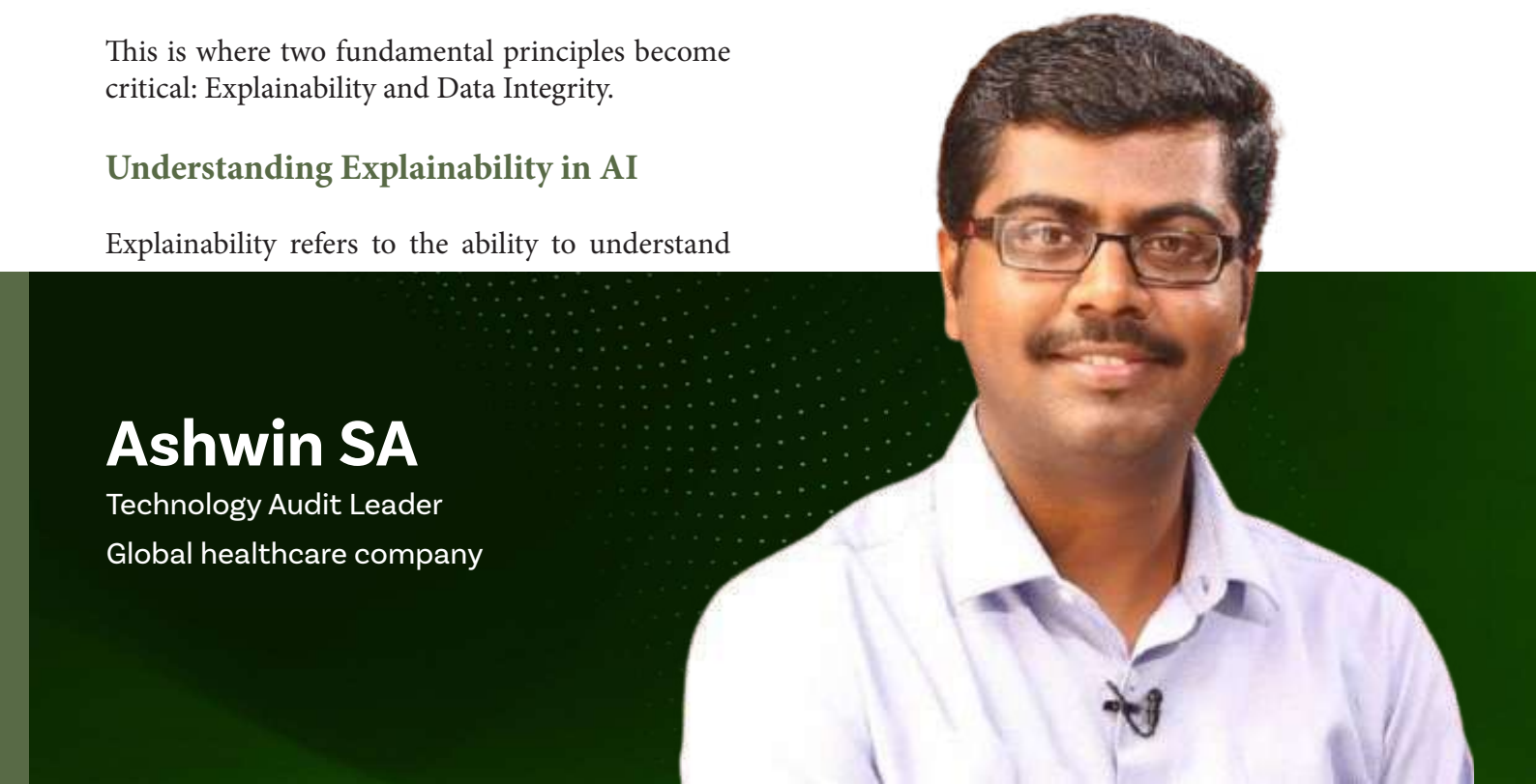
Explainability refers to the ability to understand and clearly describe how an AI system arrives at its decisions or predictions.

To understand its importance, imagine an organization using AI to approve loans. The system processes thousands of data points—income patterns, credit histories, spending behaviors—and quickly determines whether an applicant qualifies. The speed and efficiency are impressive.

But what happens when the rejected applicant asks a simple question:
“Why was my loan application denied?”

If the system cannot provide a meaningful explanation, trust begins to erode.

Explainability ensures that AI decisions are not just technically accurate but also understandable and defensible. For organizations deploying AI in high-stakes environments such as finance, healthcare, or recruitment, explainability becomes essential for maintaining transparency, fairness, and accountability.



Ashwin SA
Technology Audit Leader
Global healthcare company

The Foundation of AI: Data Integrity:

While much attention is often placed on sophisticated algorithms and powerful models, the true foundation of any AI system is data. Data integrity refers to accuracy, completeness, consistency, and reliability of the data used to train, test, and operate AI systems.

An AI model learns patterns from historical data. If that data is flawed—containing inaccuracies, missing values, or biases—the model will inevitably produce flawed outcomes. In AI-native startups, compromised data integrity can lead to serious consequences, including

- Incorrect predictions or recommendations
- Product failures
- Loss of customer trust Regulatory and legal risks

Simply put, even the most advanced AI model cannot compensate for poor-quality data.

Why These Issues Matter More for AI-Native Startups

For traditional companies, AI may be a supporting feature within a broader product or service. But for AI-native startups, AI is often the central engine driving value creation. This makes explainability and data integrity not just technical concerns—but business-critical factors.

- **Building Trust with Customers and Investors**

Startups must convince customers, investors, and regulators that their AI systems are reliable and fair. Transparent decision-making helps build credibility and encourages adoption.

- **Ensuring Reliable Product Performance**

AI systems rely entirely on data. Without strong data integrity, predictions and recommendations become unreliable, ultimately damaging the startup's reputation.

- **Meeting Regulatory and Ethical Expectations**

Governments and regulatory bodies worldwide are increasingly scrutinizing AI systems. Organizations must demonstrate that their models are transparent, unbiased, and accountable.

For startups operating in sectors like finance, healthcare, or employment, the ability to explain AI decisions is rapidly becoming a regulatory requirement.

Key Challenges AI Startups Face

Despite its importance, maintaining explainability and data integrity is far from easy. AI-native startups face several unique challenges.

- **Complexity of Modern AI Models**

Many startups rely on advanced machine learning and deep learning models. While powerful, these models often function as complex mathematical systems that are difficult to interpret. As models grow more sophisticated, understanding their internal reasoning becomes increasingly challenging.

- **Limited Access to High-Quality Data**

Startups often lack the extensive datasets available to large corporations. Gathering clean, reliable, and well-structured data can be expensive and time-consuming. Incomplete or inconsistent data can directly impact the reliability of AI outcomes.

- **Data Bias and Ethical Risks**

Historical datasets may contain hidden biases related to gender, geography, income, or demographics. If these biases are embedded in training data, the AI system may unintentionally produce unfair outcomes. Without strong explainability tools, detecting and correcting such biases becomes extremely difficult.

- **Speed vs Governance**

Startups thrive on speed. Rapid development cycles help them innovate and compete with larger players. However, this urgency can sometimes lead to weak governance practices, including limited documentation, insufficient validation, and inadequate data controls.

- **Challenges in Data Lineage and Traceability**

AI models often combine data from multiple internal and external sources. Over time, tracking where the data originated, how it was transformed, and how it influenced decisions becomes increasingly complicated. Without clear data lineage, auditing AI systems becomes significantly harder.

A Layered Approach to Auditing AI Systems

Given the complexity of AI systems, auditing them requires a structured and layered approach that examines the entire AI lifecycle.

Below is a five-layer strategy that auditors and governance teams can use to assess explainability and data integrity in AI-native startups.

Data Source and Integrity Assessment

The first layer focuses on the foundation of the AI system, the data itself. Auditors should evaluate:

- The origin of datasets (internal, external, or third-party sources)
- Data collection methods
- Accuracy, completeness, and consistency of data
- Controls preventing unauthorized data modification
- Documentation of data lineage. Ensuring reliable and traceable data pipelines is essential for trustworthy AI outcomes.

Model Design and Explainability Evaluation

The second layer examines how the AI model is designed and whether its decisions can be interpreted.

Key areas of review include:

1. Model architecture and algorithms
2. Use of explainability tools and frameworks
3. Documentation describing key decision variables
4. Selection of interpretable models where possible

The goal is to ensure that AI decisions can be understood, justified, and reviewed when necessary.

Data Processing and Model Training Controls

The third layer evaluates the processes used to prepare data and train the model. Auditors should review:

- Data cleaning and preprocessing practices
- Feature engineering methods
- Separation of training and testing datasets
- Version control for models and datasets
- Bias and fairness testing procedures

This layer ensures that the training process remains controlled, documented, and reproducible.

Decision Transparency and Output Validation

Next, auditors evaluate how AI decisions are delivered to users. Important considerations include:

1. Whether outputs include explanations or reasoning
2. The ability to trace decisions back to input variables
3. Testing for accuracy and consistency
4. Human review mechanisms for high-risk decisions

This step ensures that AI systems do not operate as unexplainable black boxes in real-world environments.

Continuous Monitoring and Governance

Finally, AI systems require ongoing oversight after deployment. Auditors should assess:

- Monitoring mechanisms for model drift
- Regular data quality checks
- Periodic explainability reviews
- Governance frameworks and accountability structures
- Incident reporting and model retraining processes

Continuous monitoring ensures that AI systems remain reliable even as data, environments, and user behavior evolve.

Moving Beyond the Black Box

AI-native startups have the potential to transform industries through intelligent automation and data-driven insights. But with that power comes responsibility.

Explainability and data integrity are no longer optional technical features—they are foundational pillars for trust, accountability, and sustainable innovation.

By embedding transparency into model design and ensuring strong data governance, startups can move beyond the "black box" and build AI systems that are not only powerful but also trustworthy and auditable.

In the rapidly evolving AI landscape, the organizations that succeed will be those that combine innovation with responsibility.

IIA India Calcutta Chapter

The IIA India Calcutta Chapter successfully organized its 33rd Annual Conference on March14, 2026, at ITC Sonar, Calcutta. The event brought together industry leaders, audit professionals, and experts .

The theme of the Conference "Internal Audit: Control- Risk - Governance and beyond.," the conference fostered engaging discussions, providing practical insights and strategies to navigate the evolving audit landscape.

The event was held under the leadership of Mr. Abin Kumar Mukhopadhyay, President, IIA India Calcutta Chapter, and Mr. Subhash Chandra Saraf ,Convenor, Conference Committee.

The Inaugural session commenced with the lighting of the lamp by dignitaries Mr Neeraj Bansal Head KPMG Global India, graced the occasion as Chief Guest, while Mr.Krishnan Venugopal, President, IIA India, was the Guest of Honour.

The Inaugural Session concluded with a vote of Thanks delivered by Mr Anupam Kumar Das, Secretary IIA I Calcutta Chapter.

The Conference had Inaugural Session, Four Technical Sessions, and panel discussion. The Conference was attended by 150 delegates.

The conference featured distinguished speakers, including:

- Mr Vivek Agarwal, Founder, Epagaar
- Mr Mukundan K V , CEO IIA India
- Ms Lalitha Satheesh, M D –Risk & Compliance Capability Lead , Accenture.
- Mr Siddheswar Bhalla, Past President IIA India
- Mr Sunil Rao Addanki, M D Protiviti India
- Mr Divya Prakash Bengani,CFO Mageba Bridge Products P Ltd
- Mr. Arpit Garg (RiskMan Consulting)
- Mr Sunirmal Talukdar Independent Director.

The Conference was a resounding success, reinforcing the importance of Global governance innovations in internal auditing and equipping professionals with insights to navigate future challenges. The event was attended by around 145 participants as well as got significant publicity in print and digital media.

Continuous Assurance

Moving from Periodic Sampling to Real-Time Cloud ERP Monitoring

Internal audit has traditionally operated on a predictable rhythm—annual plans, periodic fieldwork, and sample-based testing conducted weeks or months after transactions occur. For decades this model has provided 'reasonable' assurance over financial reporting and operational controls as mostly desired by Audit Committee and/or Senior Leadership. However, as organizations increasingly run their core processes on integrated cloud ERP platforms, the pace and volume of transactions have changed dramatically.

In today's world, risks can materialize within hours, yet assurance is often delivered later. This mismatch between the speed of business operations and the timing of assurance activities is prompting many organizations to rethink how internal audit monitors risk. Continuous Assurance (CA), enabled by analytics and real-time monitoring of ERP data(wherever available), is emerging as a powerful way to bridge this gap.

At its core, Continuous Assurance represents a shift from postmortem i.e. retrospective verification to proactive oversight and monitoring.

Periodic Sampling – what is missing?

Traditional audit methodologies rely heavily on sampling to determine whether controls operated effectively during a defined period usually the in scope audit period. While statistically sound, sampling inevitably covers only a fraction of the total transaction population because of subsampling. In large organizations processing thousands of transactions daily, this approach leaves a significant portion of operational activity outside the scope of review.

This limitation becomes particularly evident in high-volume processes such as procure-to-pay, order-to-cash, or financial close activities. A periodic audit may test a limited set of transactions, while the underlying system may have processed thousands during the same period.

As a result, many audit findings reflect issues that have occurred repeatedly before being detected. Exceptions such as duplicate payments, approval overrides, or access conflicts are often identified months after they first occurred. By that time, remediation typically focuses on correcting historical issues rather than preventing future occurrences.

Dhiraj Kumar Gupta
Deputy Manager, VOIS

In an environment where business processes are increasingly automated and transactions occur continuously, the traditional 'look-back' or 'post-mortem' model of assurance is becoming less effective.

Cloud ERP: Enabling Continuous Monitoring

The rapid adoption of cloud ERP platforms such as SAP S/4HANA, Oracle Cloud, and other integrated enterprise systems has created an opportunity to fundamentally rethink how assurance is delivered. These systems generate large volumes of structured transactional data and maintain detailed system logs that capture user activity, approvals, and system changes. These systems generate large volumes of structured transactional data and maintain detailed system logs that capture user activity, approvals, and system changes. This opportunity is particularly relevant in Global Capability Centers and shared services environments, where large transaction volumes and standardized processes make population-level monitoring both practical and highly impactful. When combined with analytics and automated monitoring rules, this data can provide continuous insight into control performance and effectiveness.

Continuous Assurance frameworks typically rely on automated routines that scan transaction populations against defined risk parameters. Examples include:

- Identification of duplicate vendor payments
- Monitoring of manual journal entries outside defined thresholds
- Detection of segregation-of-duties conflicts in user access
- Alerts for unusual purchasing or payment patterns

Unlike traditional audit procedures, which rely on periodic testing, these monitoring rules can operate daily or even in near real time. This enables internal audit and management to identify anomalies quickly and respond before control breakdowns escalate into larger issues.

In effect, Continuous Assurance allows auditors to evaluate the full population of transactions rather than a limited sample.

From Control Testing to Control Monitoring

A key conceptual shift in Continuous Assurance is the transition from testing controls to monitoring controls.

Traditional audits validate whether controls operated effectively during a defined time period. Continuous monitoring, by contrast, evaluates control performance continuously by analyzing transactional data streams.

In practice, automated monitoring rules analyze the entire population of transactions rather than

a limited sample. These rules identify anomalies or transactions that fall outside predefined control parameters, allowing auditors and process owners to focus their attention on investigating exceptions rather than reviewing every transaction manually.

Automated monitoring rules can identify patterns that would be difficult to detect through manual testing. Instead of spending significant time selecting samples and verifying documentation, auditors can focus their efforts on investigating exceptions and understanding the underlying causes.

This approach allows internal audit to move closer to the organization's operational heartbeat, providing insights that are both timely and actionable.

In practice, many organizations begin their Continuous Assurance journey with high-risk processes such as procure-to-pay, user access management, or financial reporting. As monitoring frameworks mature, coverage can expand across additional operational areas.

A Practitioner Perspective

A global manufacturing company transitioning to a cloud-based ERP environment recently implemented automated monitoring across its procure-to-pay process. Historically, internal audit reviews frequently identified recurring exceptions related to duplicate invoices and approval overrides. As part of a Continuous Assurance initiative, the organization deployed monitoring rules that scanned the full population of transactions daily. Potential duplicate payments, unusual vendor master changes, and high-value payment overrides were flagged automatically and routed to process owners for review.

Within the first year, internal audit observed a notable reduction in repeat audit observations in the procure-to-pay cycle. More importantly, many potential control issues were identified and resolved during routine operations rather than being discovered months later during traditional audit fieldwork.

For the audit function, this also changed the nature of conversations with management—from explaining historical findings to collaboratively addressing emerging risks.

Strengthening the Partnership Between Audit and Operations

Continuous Assurance also has an important cultural impact. Traditional audits sometimes identify issues long after the relevant transactions have occurred, which can create frustration among operational teams.

Real-time monitoring shifts this dynamic. When exceptions are detected quickly and shared with process owners, corrective action can be taken while the issue is still fresh in the system.

Over time, this approach strengthens accountability for controls within the business and reinforces internal audit's role as a partner in improving governance and operational discipline.

Implementation Considerations

Adopting Continuous Assurance requires thoughtful implementation. Organizations must address questions around data access, integration with ERP systems, and the design of monitoring rules. Clear governance structures are also needed to define who reviews alerts and how exceptions are resolved.

Audit teams themselves must adapt by strengthening capabilities in data analytics, ERP architecture, and technology-enabled auditing techniques. However, many organizations have demonstrated that a phased approach—starting with a small set of high-impact monitoring rules—can deliver meaningful results quickly.

The Future of Assurance

Continuous Assurance represents a natural evolution in the internal audit profession. As organizations digitize their operations and transaction volumes increase, stakeholders expect assurance functions to provide more timely insights into emerging risks.

By leveraging ERP data and analytics-driven monitoring, internal audit can move beyond retrospective reviews and position itself closer to the flow of business activity.

Ultimately, the goal of internal audit has always been to provide confidence that controls are operating effectively. In a digital enterprise where transactions occur instantly, assurance must evolve to keep pace. Continuous Assurance ensures that internal audit is not simply reviewing the past, but actively safeguarding the present—and helping organizations anticipate the risks of tomorrow.

IIA India Madras Chapter

The Annual Conference 2026 – IIA Madras Chapter, held on 27th & 28th February 2026 from 09:00 AM to 05:00 PM at Hilton Chennai, was a comprehensive and insightful two-day event centered around the theme "Internal Audit at the Inflection Point." The conference brought together a distinguished lineup of industry leaders, audit professionals, technology experts, and legal practitioners to deliberate on the evolving landscape of internal audit.

The sessions featured eminent speakers including Lakshminarayanan D, Charanjoth Singh Nanda, Vijay Nadadur, Sureshbabu D, and M. S. Bharath, among many others. Their discussions highlighted critical themes such as digital transformation, ESG integration, cybersecurity risks, regulatory challenges, and the future of internal audit functions.

Key insights were shared by experts like Sathyananda Prabhu, Elango Yeasaiyan, Aparna Rao, and S. Ramakrishnan, focusing on risk management, governance frameworks, and emerging cyber threats. ESG perspectives were addressed by Poonam Joshi and Niharika Sharma, emphasizing sustainability and responsible business practices.

The conference also featured engaging sessions from industry leaders such as Sweta Agarwal, Raman Krishnan, Arjun Prathap, Harini S, and Krishna Srinivasan, who shared practical insights on audit innovation, automation, and strategic decision-making.

A special interactive segment, moderated by Ravi Veeraraghavan, added depth through engaging discussions with industry practitioners. Additional contributions from speakers like Ganesh Sankararaman, Yogeshwaran Sundaresan, and Revathi Raghunathan further enriched the knowledge-sharing experience.

With 285 participants attending physically, the conference successfully fostered collaboration, knowledge exchange, and professional networking. Spanning 12 hours of curated sessions, it provided valuable perspectives on how internal audit functions can adapt and thrive at a critical transformation point.

Overall, the event was a resounding success, equipping professionals with forward-looking insights and practical strategies to navigate the dynamic risk and compliance environment

Valuation Scrutiny in Stress Cycles

The Internal Auditor's Role in Down-Rounds and Secondary Sales

In today's capital environment, valuation is no longer a narrative of continuous growth, it is a test of resilience. Across geographies, down-rounds and secondary sales have become increasingly visible as markets recalibrate. India has witnessed notable valuation corrections in recent years such as Byju's marking down its valuation amid funding challenges, and Swiggy raising capital at a lower valuation than its previous peak during the funding slowdown. At the same time, secondary transactions have gained traction across growth-stage startups. While these transactions are commercially valid, they introduce significant risk in fair value measurement making them a critical focus area for internal auditors.

Understanding the Context

A down-round occurs when a company raises capital at a valuation lower than its previous funding round. A secondary sale, on the other hand, involves existing shareholders selling their stake often without fresh capital infusion into the business. Both scenarios introduce complexities in fair value assessment, especially when they challenge prior valuation benchmarks.

For internal audit, the objective is not to determine valuation, but to answer a far more important question: "Are valuation conclusions built on disciplined processes, unbiased assumptions, and robust governance or are they influenced by pressure, optics, and selective interpretation?"

When Transaction Price Misleads

A recurring issue in practice is the over-reliance on the latest transaction price as a proxy for fair value. However, under IFRS 13 / Ind AS 113, fair value reflects an orderly transaction between market participants, not every transaction.

Consider two scenarios:

- A startup raises funds at a lower valuation after engaging multiple institutional investors during a market downturn. This likely reflects fair value aligned with market correction.
- A founder executes a secondary sale to a single investor at a discounted price due to personal liquidity needs. This may not represent fair value, as it lacks market depth and competitive discovery.

Aayush Bajaj
CA, CIA, CPA US
Grevx Consulting

The internal auditor's role is to independently verify whether the transaction is truly representative or merely convenient for narrative setting.

The Real Risk: Management Bias, Not Models

Valuation failures rarely arise from flawed models they arise from biased assumptions.

In down-rounds and secondary transactions, management incentives are often complex:

- Avoiding signaling risk to the market
- Protecting ESOP valuations
- Managing investor perception
- Deferring impairment recognition

These pressures can subtly influence:

- Selection of valuation methodologies
- Optimism in projections
- Justification for ignoring unfavorable transactions

Internal auditors must therefore go beyond numbers and ask:
What is driving the valuation conclusion? Economics or incentives?

Where Internal Auditors Must Challenge

1. Nature of the Transaction

Internal auditors must verify whether the transaction is orderly:

- Was there sufficient market exposure?
- Were multiple independent parties involved?
- Was there genuine price discovery?

Evidence should be drawn from board minutes, investor outreach records, and deal negotiations not just management assertions.

2. Consistency of Valuation Approach

A common red flag is methodological inconsistency. Auditors must challenge:

- Why is the latest funding round being used despite market shifts?
- Why has a DCF approach been selectively introduced or removed?
- Are valuation methods consistent with prior periods and industry practices?

In practice, valuation approaches are sometimes changed to support desired outcomes, rather than reflect underlying economics.

3. Assumptions vs. Reality

The most powerful audit test is comparison:

- Do valuation projections align with board-approved budgets?
- Are they consistent with recent actual performance?
- Are discount rates reflecting current risk environments?

A frequent audit finding: projections used for valuation are often more optimistic than those used internally for planning. This disconnect is a clear indicator of bias.

4. Capital Structure and Economic Reality

Down-rounds often include structured terms liquidation preferences, anti-dilution rights, or convertible instruments that distort headline valuation.

For example:
A company raises capital at a reduced valuation but grants strong downside protection to new investors. While the headline valuation appears reasonable, the economic value of common equity may be significantly lower.

Internal auditors must ensure:

- Proper allocation of value across share classes
- Appropriate use of models such as OPM or PWERM
- Full consideration of investor rights in valuation conclusions
- Failure to do so can materially misstate fair value.

5. Secondary Transactions: A High Skepticism Zone

Secondary sales require heightened scrutiny because they are often:

- Limited in participation
- Liquidity-driven
- Negotiated without broad market exposure

Internal auditors must challenge:

- Why was this transaction considered representative of fair value?
- Were control premiums or discounts appropriately applied?
- Is management selectively using this transaction to support valuation conclusions?

In several real-world cases, selective secondary transactions have been used to avoid valuation markdowns, highlighting the need for strong audit challenge.

Five Questions Every Internal Auditor Must Ask

To move from review to real scrutiny, internal auditors should consistently ask:

- Why are valuation assumptions more optimistic than internal budgets?
- What evidence supports the transaction being orderly and market-driven?
- Why was this valuation method chosen over alternatives?
- How do investor rights impact the true economic value of equity?
- Where could management bias have influenced the outcome?

These questions often reveal more than the valuation model itself.

Governance: The True Control Layer

The strength of valuation lies in governance, not computation.

Internal auditors should assess:

- Independence and competence of valuation experts
- Controls over selection of comparables and key inputs
- Documentation of assumptions and judgments
- Challenge mechanisms at management and board levels
- Consistency across financial reporting, investor communication, and internal planning

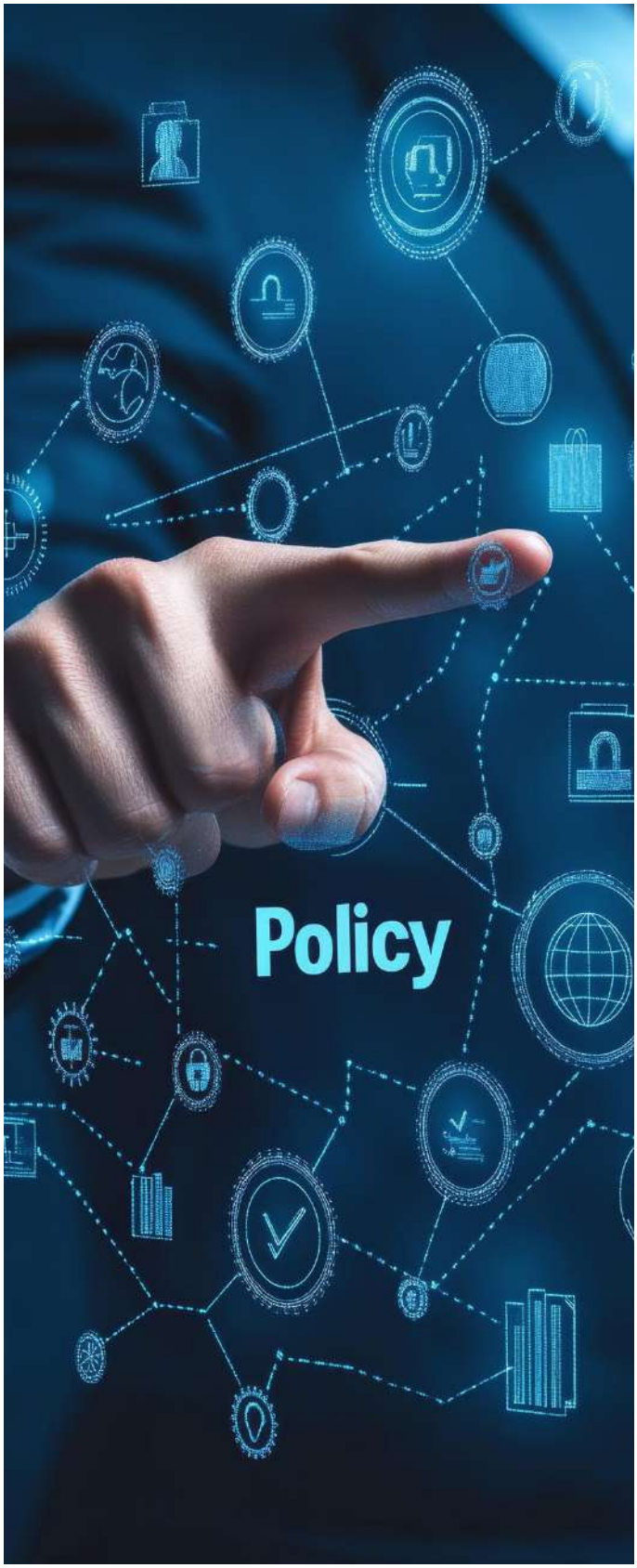
Weak governance not technical complexity is the root cause of most valuation issues.

Conclusion: Challenging Certainty

Down-rounds and secondary sales are not inherently problematic they reflect market reality. The real risk lies in unquestioned assumptions presented as objective conclusions.

Internal auditors must move beyond procedural review to intellectual challenge. Their role is not to dispute market movements, but to ensure that valuation conclusions are evidence-based, unbiased, and consistently applied.

Because in valuation, the greatest risk is not volatility it is certainty without challenge.



Agentic Audit

Transitioning from Automated Testing to Autonomous AI Audit Workflows

Internal audit has spent the better part of a decade learning how to automate tasks. Robotic process automation extracts evidence. Scripts compile workpapers. Dashboards alert when a threshold is breached. These are genuine advances — they have improved efficiency and consistency in ways that matter.

But there is a distinction that gets lost in conversations about automation, and it matters enormously for where the profession is heading. Automating individual tasks is not the same as automating the audit workflow itself. In virtually every organisation today, a human still decides what to test, triggers each procedure, and determines what to do when the output arrives. The orchestration of audit work — the judgment about what warrants attention, when, and why — remains entirely human. Automation has made individual steps faster. The architecture of how assurance is delivered has not fundamentally changed.

Agentic AI changes that architecture. This article explores what that transition means in practice — what autonomous audit workflows look like, what the journey toward them actually requires, and what every CAE should be asking right now that most are not.

Automation and Autonomy: Understanding the Difference

A well-designed RPA bot is deterministic. It follows a defined sequence and stops when something unexpected appears. It executes exactly what it was told to do, and nothing more. An AI agent operates differently — it can pursue a multi-step objective with contextual reasoning, adapting its path based on what it finds. In an audit context, this means a system that continuously monitors enterprise data, detects when a condition warrants attention, decides what evidence is relevant, retrieves it across multiple systems, and assembles a structured finding — all without a human initiating each step. The human enters the process not at the beginning, but where professional judgment is genuinely required: validating the finding, assessing its significance, and determining the response.

This is the transition this article describes. Not incremental automation — a different model for how assurance is delivered. Figure 1 illustrates how the progression from task automation to autonomous workflows changes both what the system does and what the auditor does.

Mallesh Bulusu
Internal Audit & SOX Leader

Figure 1 — Agentic Audit Maturity Model

Stage	How the Workflow Operates	Where the Auditor Focuses
Task Automation (RPA)	Bots execute defined procedures — pull evidence, apply sampling criteria, assemble workpapers. Each step triggered by a human.	Designing tests, triggering bots, reviewing outputs, interpreting exceptions.
AI-Assisted Analytics (Augmented)	ML detects anomalies across full populations. GenAI drafts risk statements, attributes, and gap analyses. Humans still initiate investigation.	Reviewing AI-flagged exceptions, applying judgment to outliers, directing next steps.
Autonomous AI Workflows (Agentic)	AI continuously monitors enterprise data. On detecting a risk signal it initiates investigation, gathers evidence across systems, and assembles a finding — without waiting to be asked.	Validating AI-assembled findings, applying professional judgment, communicating risk conclusions to leadership.

The critical shift between Stage 2 and Stage 3 is not the sophistication of the technology. It is who initiates the audit workflow. In autonomous environments, risk signals initiate investigation. The auditor validates conclusions rather than orchestrating procedures.

What the Automation Journey Has Already Taught Us

The path toward agentic audit is a progression, not a sudden leap. Our team began deploying RPA bots for SOX testing in 2021 — retrieving system logs, applying sampling criteria to control populations, pulling approval records, and assembling workpapers end to end. Alongside this, we developed Continuous Controls Monitoring scenarios for manual journal entry testing and duplicate invoice detection, each operating as a live analytical monitor rather than a periodic test.

The efficiency gains were real. But the more significant outcome was what happened to auditors' attention once the mechanical work was handled. When the team stopped spending time gathering evidence, they started reading it differently — asking harder questions, following anomalies further, engaging more deeply with what the data was actually telling them. Automation did not just save time. It redirected attention toward the work that genuinely requires a trained professional.

One outcome in particular shaped how I think about this. When we shared the duplicate invoice population view with business teams, they took ownership of it. That dashboard is now reviewed before every payment run — not by the audit function, but by the business itself. The control shifted from something auditors tested periodically to something embedded in daily operations. That shift — from retrospective testing to continuous, business-owned monitoring — is exactly what autonomous AI workflows promise to accelerate across the broader control environment.

By 2025, we had extended into AI-assisted capabilities: generative AI drafting risk statements, audit attributes, assertions, audit findings, and control gap analyses etc., The next phase, currently under active development, involves converting existing bots into agentic workflows — systems that move from detecting a risk signal to gathering evidence to assembling a finding for auditor review, without a human orchestrating each step. The ambition is clear. The reality, as I will come to, is more complicated than the vision suggests.

What Autonomous AI Audit Workflows Look Like

In a SOX controls environment, a mature autonomous audit workflow operates continuously. An AI agent monitors ERP transaction logs, access management records, and reconciliation data. When it detects a condition outside established control parameters — a journal entry pattern

deviating from normal behaviour, a segregation-of-duty conflict, a reconciling item ageing past defined thresholds — it does not simply alert. It initiates investigation: retrieves transaction history, extracts access logs, cross-references the control matrix, and assembles a structured preliminary finding with a risk score and full evidence trail. That package is placed in front of an auditor with a specific request: apply your judgment to this.

This model is already in production in adjacent fields. AI agents in financial crime compliance perform exactly this workflow — monitoring transactions, building cases from multiple data sources, surfacing them for human review. Dedicated audit platforms are now bringing the same model to the assurance function, with agents that follow audit plans end to end, perform control tests, and generate documented workpapers while keeping auditors in the loop for final conclusions. Enterprise workflow platforms are accelerating this shift from a complementary direction — embedding agentic AI directly into the operational systems where work already happens, so that autonomous audit and risk workflows operate within the same environment as the business processes they monitor, rather than sitting alongside them as separate tools. KPMG's 2025 research on the agentic shift in SOX describes this convergence as capable of transforming SOX from a periodic compliance exercise into continuous strategic risk management. A 2025 AuditBoard survey of over 2,500 auditors found 64 per cent actively exploring AI agent adoption, with controls testing identified as the highest-value application.

Figure 2 — Autonomous AI Audit Workflow

ZONE A — AI EXECUTION (steps 1–4, system-initiated)		
1	**Continuous data monitoring**	ERP transactions, access logs, reconciliation data — always on, no human trigger required.
2	**Risk signal detected**	Anomaly, threshold breach, or control deviation identified across the monitored population.
3	**Multi-system evidence gathering**	Agent retrieves transaction history, access logs, and control matrix across connected systems.
4	**Finding assembled & risk-scored**	Structured preliminary finding with full evidence trail and risk score presented to auditor.
ZONE B — AUDITOR OVERSIGHT (steps 5–7, judgment-led)		
5	**Auditor review & judgment**	Is this a genuine control failure or an explainable business condition? Auditor decides.
6	**Escalation decision**	Determine severity, ownership, and appropriate response path.
7	**Resolution & reporting**	Communicate findings to management; close or escalate; update control record.

Steps 1–4 are AI-initiated and AI-executed. Steps 5–7 are auditor-led. The handoff — AI assembles, auditor concludes — is where professional judgment remains non-negotiable.

The Honest Complexity: Where the Vision Meets Reality

Here is the part that does not appear in the optimistic literature about agentic AI in audit, but that every practitioner building toward this model will recognise immediately.

The most significant barrier to deploying autonomous audit workflows is not the AI itself — it is enterprise architecture. The systems that hold the most critical control evidence were not designed with AI agents in mind. RPA bots could work around this because they mimic user actions: they navigate, click, and extract the way a human would. AI agents need something different — structured, programmatic access through APIs that do not always exist, across integration layers that many enterprise vendors have not yet opened. Third-party systems that sit at the heart of most SOX programmes remain, for now, a meaningful constraint on how far autonomous workflows can reach. This is not a

reason to delay the journey. It is a reason to plan it honestly and engage technology vendors as a strategic priority rather than an afterthought.

Security governance presents a second layer of complexity. Autonomous systems create access risks that scripted bots do not. A bot operates with fixed credentials and a defined scope. An AI agent's access can expand dynamically based on the task it is pursuing. Without identity governance designed specifically for AI agents — least-privilege principles, short-lived credentials, real-time activity logging — autonomous systems can traverse data boundaries that no human auditor would be permitted to cross. CyberArk's 2025 research found machine identities now outnumber human identities by 82 to one in large enterprises, with fewer than half of organisations applying formal governance policies to them. OWASP identifies prompt injection as the leading AI security vulnerability (LLM01:2025) — the risk that malicious content within data manipulates an agent's actions. For audit functions, human review of AI-assembled findings is therefore not a bureaucratic formality. It is a governance control.

Building effective guardrails — defined boundaries on what an agent can access, what actions it can take, and what requires human approval before proceeding — is not optional governance hygiene. It is the foundational design requirement for any autonomous audit workflow.

A third consideration is specific to audit: every finding must be defensible. An AI agent that surfaces an anomaly but cannot reconstruct its reasoning in terms a process owner, external auditor, or regulator can evaluate does not produce a finding — it produces a hypothesis. The complete evidence chain must be logged and reconstructable independently of the AI output. This is a design requirement, not an afterthought.

What This Means for the Auditor's Role

The question that arises in every conversation about AI in audit is some version of: does this replace auditors? It is the wrong framing. The more precise question is what the auditor's contribution looks like when AI handles the orchestration of audit work.

The honest answer is that the work becomes more demanding, not less. When autonomous systems continuously surface evidence-backed findings for human review, auditors are no longer asked to gather the evidence — they are asked to judge it. The judgment calls that remain are the genuinely difficult ones: distinguishing a control failure from an explainable business condition, assessing whether a pattern is systemic or isolated, deciding how to communicate a finding in a way that drives the right response. These require experience, organisational understanding, and professional accountability that no AI system delivers reliably.

What changes is how that expertise is applied — less time on evidence collection, more time on interpretation, control advisory, and strategic risk dialogue. For audit functions that have already made the automation investment, this shift is already visible. It points clearly toward where the next investment should go: not more bots, but more capable auditors working alongside more capable systems.

Conclusion: One Question for Monday Morning

The internal audit profession is at a genuine inflection point. The task automation of the last decade has been valuable, but it has not changed the fundamental architecture of how assurance is delivered. Autonomous AI workflows change that architecture — moving from periodic, human-orchestrated procedures toward continuous, intelligence-driven risk monitoring where AI handles the groundwork and auditors apply the judgment that matters.

The transition is more complex than the vision suggests. Enterprise integration constraints are real and require sustained engagement with technology vendors. Governance design matters enormously — credential management, access controls, and explainability requirements must be built in from the start. The organisations that will lead the next decade of assurance are those investing now — in automation foundations, governance frameworks, and auditor capabilities — before the shift fully accelerates. The goal is not a world where AI does the audit. It is a world where AI does the work that has been keeping auditors from doing the audit properly.

Here is the question every CAE should bring to their automation lead this Monday: "If I asked our systems to trigger an audit investigation today — without a human starting it — which of our critical control systems could actually support that? And for the ones that cannot: is the barrier the technology, the vendor, or our own governance?" Most audit functions will find the answer uncomfortable. That discomfort is exactly where the real work begins.

WOMEN'S FORUM

Stillness in the Storm: How Women Auditors Can Balance Ambition with Inner Well-being

In the fast-paced world of audits, deadlines, and decisions, stillness often feels like a luxury. For the modern woman auditor, life is a constant juggle—between professional excellence and personal responsibilities, between ambition and expectations, between giving to others and finding time for oneself. The calendar is full, the mind is fuller, and somewhere in between, well-being quietly takes a back seat.

But what if the answer to managing this constant motion is not doing more—but learning to pause? This is where the ancient wisdom of yoga and meditation becomes not just relevant—but essential.

The Reality of the Multitasking Woman

Women today are natural multi-taskers—not by choice alone, but often by necessity.

A woman auditor may start her day reviewing reports, attend back-to-back meetings, manage teams, respond to urgent queries—and still return home to take care of family, relationships, and personal commitments.

This constant switching of roles comes with an invisible cost:

- Mental fatigue
- Physical strain
- Emotional exhaustion

Over time, this leads to reduced focus, irritability, and burnout—something many professionals silently experience but rarely acknowledge.

The question is not whether women are capable of handling it all—they are.
The real question is: At what cost?

Yoga: More Than Just Physical Exercise

Yoga is often misunderstood as just a form of physical fitness.

In reality, it is a holistic practice that brings together:
- Body (Asanas)
- Breath (Pranayama)
- Mind (Meditation)

For a professional constantly operating under pressure, yoga offers something invaluable, balance from within.

It does not demand hours. Even 20–30 minutes a day can create a noticeable shift, in energy, clarity, and emotional stability.

Simple Asanas for Everyday Balance

For busy professionals, the key is not complexity—but consistency.

Here are a few simple yet powerful asanas that can easily be integrated into a daily routine:

1. Tadasana (Mountain Pose) – For Stability and Posture

A simple standing posture that improves alignment and grounding.

It helps in reducing fatigue caused by long hours of sitting or standing.

2. Bhujangasana (Cobra Pose) – For Energy and Spine Health

Perfect for those who spend long hours at desks.
It strengthens the back and opens up the chest, improving breathing and reducing stiffness.

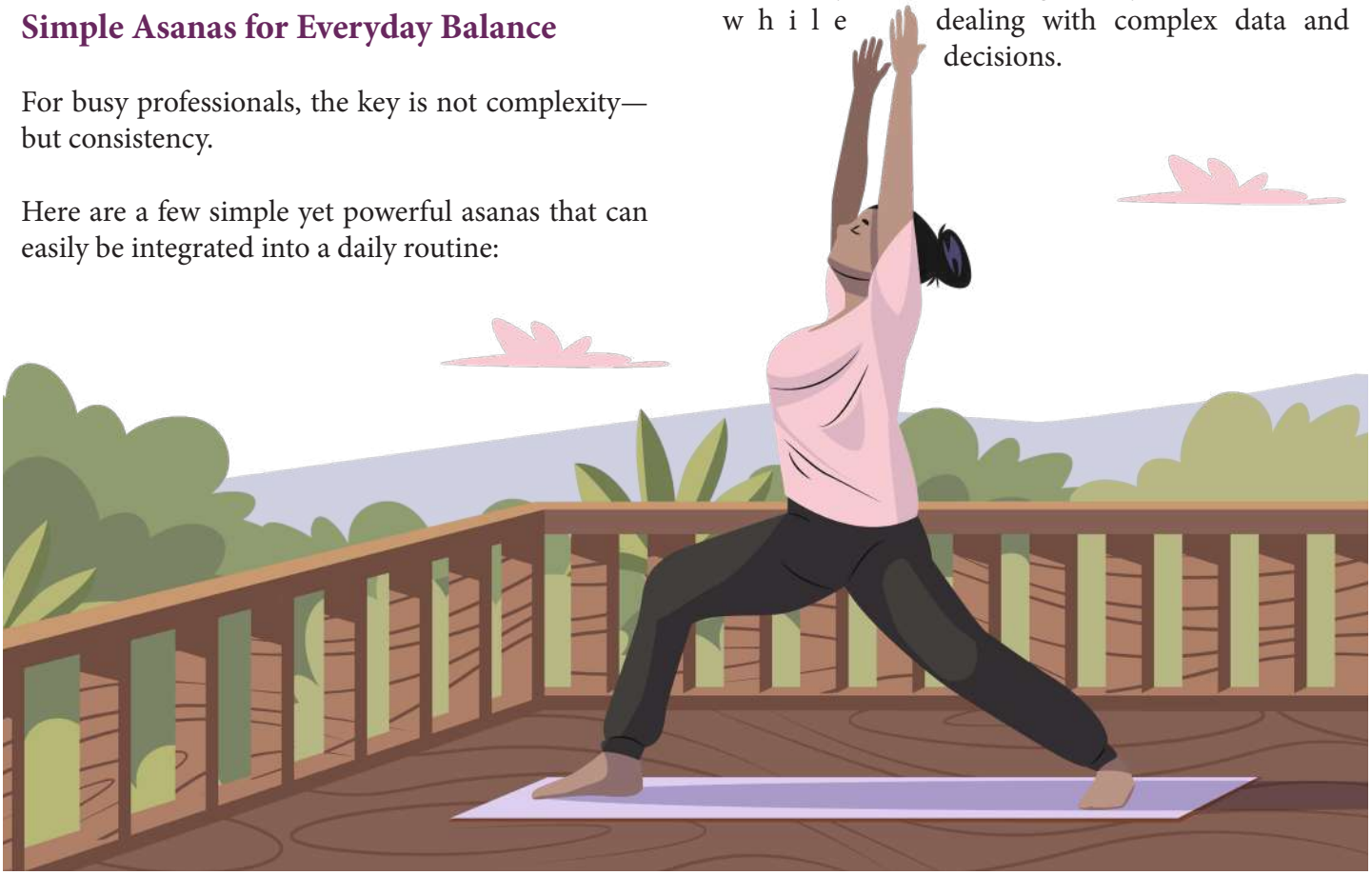
3. Balasana (Child's Pose) – For Relaxation

A deeply calming posture that helps release tension from the back, shoulders, and mind.

Even a few minutes in this pose can reset your energy.

4. Vrikshasana (Tree Pose) – For Focus and Balance

This posture enhances concentration and mental clarity — something every auditor needs while dealing with complex data and decisions.



5. Anulom Vilom (Breathing Practice) – For Mental Calmness

A simple breathing technique that balances the nervous system and reduces stress instantly.

These are not just exercises—they are tools to reconnect with oneself.

Meditation: The Power of Pause

If yoga aligns the body, meditation aligns the mind. In a profession where attention to detail, judgment, and clarity are critical, meditation can be a game-changer.

Just 10 minutes of daily meditation can:

- Improve focus and decision-making
- Reduce anxiety and overthinking
- Enhance emotional resilience
- Bring a sense of calm amidst chaos

Meditation is not about stopping thoughts, it is about learning to observe them without being overwhelmed.

For a woman juggling multiple responsibilities, this ability to pause and reset is invaluable.

Integrating Wellness into a Busy Schedule

One of the biggest misconceptions is: *"I don't have time."*
The truth is—wellness does not require extra time. It requires intentional time.
Here's how women professionals can realistically integrate it:

Start Small

- 10 minutes of stretching in the morning
- 5 minutes of deep breathing before starting work

Micro Breaks During the Day

- Step away from the screen
- Practice 2 minutes of mindful breathing
- Stretch your neck and shoulders

Create a Ritual

Instead of seeing yoga as a task, make it a non-negotiable ritual, like brushing your teeth.

Digital Detox Before Sleep

A calm mind at night leads to a productive day ahead.

From Burnout to Balance

The modern work culture often celebrates hustle,

but rarely talks about sustainability.

True success is not about how much you can push yourself, it is about how long you can sustain your energy, passion, and clarity.

Women auditors, especially in leadership roles, are not just managing work, they are managing people, expectations, and outcomes.

Without inner balance, external success starts to feel exhausting.

Yoga and meditation help shift this equation:
- From stress to stability
- From chaos to clarity
- From burnout to balance

A Message to Every Woman Professional

You do not need to prove your strength by pushing yourself endlessly.

Your strength also lies in:
- Knowing when to pause
- Taking care of your mind and body
- Choosing sustainability over exhaustion

You give your best to your work, your teams, and your family.

It is equally important to give something back, to yourself.

Because when you are balanced, everything around you becomes better.

Leadership Begins Within

As women move into leadership roles in audit and beyond, there is an opportunity to redefine what success looks like.

Not just high performance, but holistic performance. Leaders who prioritize well-being:

- Make better decisions
- Build healthier teams
- Create sustainable work cultures

When you embrace wellness, you don't just transform your life, you influence those around you.

Conclusion: Finding Stillness in Motion

Life may not slow down. Deadlines will continue. Responsibilities will grow.

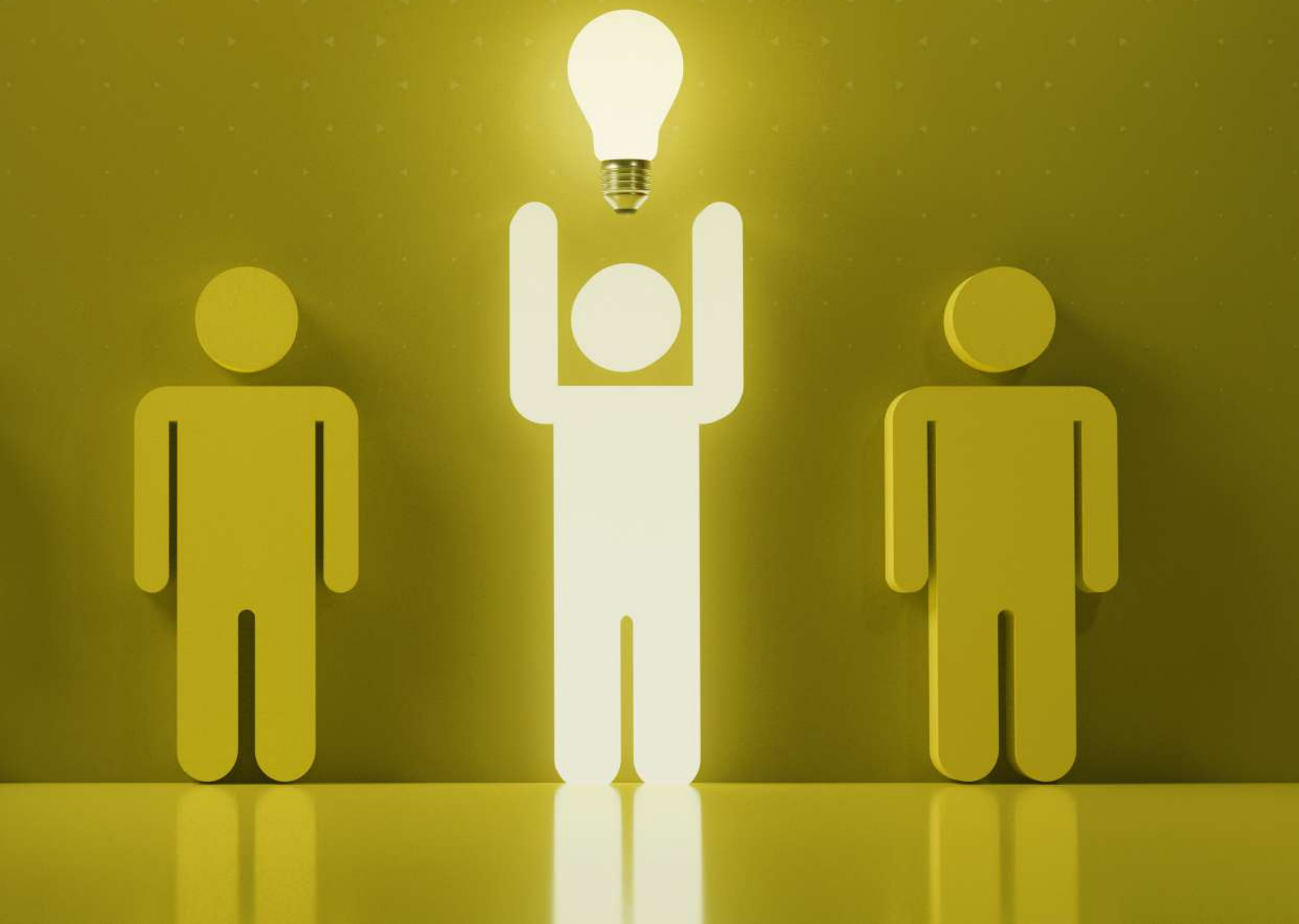
But within this constant movement, you can create your own space of stillness.

A few minutes of yoga.
A few moments of mindful breathing.
A conscious pause in a busy day.
That is all it takes to begin.

Because balance is not something you find—it is something you create.

And perhaps, the most powerful audit you will ever conduct…
is the one within yourself.

EMERGING MINDS STUDENT'S FORUM



MONITOR NEW ECONOMY

The Future of Assurance in Start-ups, Unicorns and High Growth Enterprises

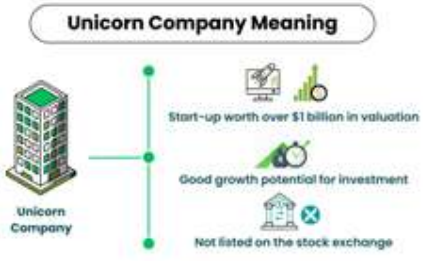
Prajakta Buggewar & Shiva Raj Katari
Global Risk Management Institute

Introduction: When Growth Outpaces Governance

Startups and unicorns have exploded over the last 10 years, transforming every industry from fintech to healthtech to quick commerce and AI platforms. With more than 100 unicorn births in the last decade alone (DPIIT, 2024), India has become one of the largest startup ecosystems in the world. But there haven't just been valuation surges and hyper-growth narratives; along with that there have also been governance failures in some high-profile startups — both across the globe as well as domestically — which epitomized a pattern that is fast becoming evident: growth has often outrun governance.

This new economy embodies a paradox for internal audit leaders. Startups are engines of innovation, and their control environments tend to be adaptable, informal, and founder-led. Traditional audit approaches — rooted in stable, process-heavy enterprises — may fall short when it comes to the velocity and digital intensity of high-growth companies, as well as funding pressures.

Auditing the new economy thus requires not incremental adaptation, but structural reimagining.



Understanding the New Economy Risk Landscape

Compared to legacy companies, high-growth companies exhibit fundamentally different characteristics relative to five key factors:

- **Speed vs Structure:** Start-ups typically prioritize speed to market over building controls. The majority of controls are established after the fact with rapid geographic and product line expansion resulting in fragmented operational processes and a lack of consistency in the maturity of operational controls.

- **Founder-Centric Decision Making:** Due to the concentration of power and informal governance structures of start-up companies, the segregation of duties and oversight mechanisms may be weakened.

- **Core Technology Infrastructure:** Due to the nature of their technology stack (cloud-native, API integrations, AI-powered decision support systems, outsourced SaaS providers), start-ups face increased risk associated with cyber security and third parties (NIST, 2018).

- **Revenue Recognition and Valuation Pressure:** Investor/prospect expectations and rounds of funding introduce risks associated with revenue recognition, manipulated KPIs, and the integrity of performance reporting.

- **Regulatory Uncertainty:** Starting companies often operate in a regulatory grey area — particularly in fintech, edtech, cryptocurrencies, and platform-based models — and the regulatory framework governing these industries is subject to change.

Agile Assurance with Traditional Audit

3.1 Early Integration of Risk at the Growth Curve

In an early stage company, many view internal audit as being either too early or 'too bureaucratic'. Best practices indicate that early introduction of sufficiently sized governance/controls for the size of the business (i.e., appropriate governance that coincides with the principles of internal control defined in COSO) is prudent.

- Conduct risk assessments based on the company's maturity.
- Evaluate financial reporting integrity along with monitoring cash burn and access control security features.
- Implement maker/checker controls for key financial and system-related workflows.
- Have audit oversight at the board level even prior to IPO planning activities.

Establishing early governance can result in saving significant remediation costs in later phases of the business lifecycle, particularly during due diligence or preparations for IPO.

3.2 Continuous Auditing with a Data-Driven Approach

High-growth businesses have a digital operating model. Therefore, the internal audit function should also reflect this digital DNA. Internal audit functions should install continuous data monitoring:

- Continuous Control Monitoring
- API Based Data Extraction
- Automated Anomaly Detection
- Key Risk Indicators (KRI) Dashboard – Real-Time Display

For example, there can be ongoing monitoring of quarter-end spikes in revenue through the use of sales logs; excess log entries for override changes from the ERP system; and exceptions related to privileged user access.

3.3 Evaluating Financial Models — More Than Just Revenue

Unicorn startups typically use narrative valuation methods based on metrics like Gross Merchandise Value (GMV), Customer Acquisition Cost (CAC), Lifetime Value (LTV), and Burn Rate. From an Internal Audit perspective, a review includes:

- Review of the reliability of KPI calculations.
- The appropriateness of assumptions used in Financial Forecasts.
- Implementation and capitalization of policies related to technology development costs.
- The appropriateness of revenue recognition in subscription and/or marketplace business models.
- The appropriateness of related party transactions and transparency in ESOP accounting.

Domain literacy will become a core competency of the audit function.

3.4 Strengthening Governance While Not Stifling Innovation

In the world of auditable start-up companies, the hardest area for an auditor to deal with is cultural sensitivity. Many companies will resist implementation of controls that may seem overly rigid.

- Make use of a strategic advisory 'touch' to the Internal Audit function.
- Utilize a 'heatmap' approach for assessing risk instead of a compliance-centered checklist.
- Design Controls with scalability in mind.
- Position risk mitigation as a means to protect value, not create bureaucracies.

Figure 2: Internal Audit Transformation – Strategic Advisory Role

Governance by Growth Stage

Governance of start-ups should evolve over phases. This lifecycle-based approach aligns assurance with maturity:

Growth Stage	Audit Focus
Seed / Early	Cash management, fraud risk, access controls
Series A / B	Process formalization, vendor governance, KPI reliability
Pre-IPO	SOX/IFC readiness, board reporting, enterprise risk management
Post-IPO	Regulatory compliance, ESG assurance, cyber resilience

Third-Party and Cloud Risk: The Invisible Perimeter

Most of the start-ups use third-party services such as cloud hosting, payment processing, analytics, HR SaaS, outsourced development teams, and other infrastructure solutions. A robust Third-Party Risk Management (TPRM) process must include:

- Review of SOC 1 / SOC 2 reports
- Monitoring service levels
- Ensuring compliance with data localization laws
- Validation of all APIs through security assessment
- Testing incident response plans

The evolving data protection regime in India and global standards such as ISO 27001 require that internal audit help ensure that the use of third parties does not erode accountability. Cyber resilience has changed from an IT risk to an enterprise viability risk.

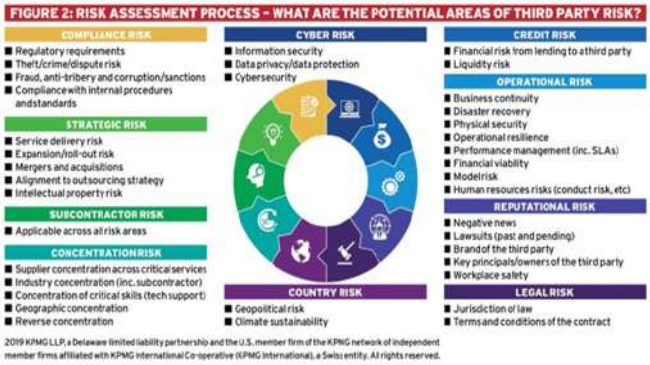


Figure 3: Third-Party Cyber Risk Management Framework

ESG and Reputation Risk in Unicorns

With the increasing importance placed on governance, sustainability and ethics, investors are beginning to assess start-ups based upon ESG disclosures, diversity metrics, and environmental footprint reporting. The following should be part of an audit leader's review:

- The accuracy of ESG disclosures
- The governance of AI and algorithmic bias
- The use of data privacy practices
- The processes for whistle-blowing
- Board of director independence

Reputation degradation happens much more quickly in the digital world since there is social amplification and immediate exposure.

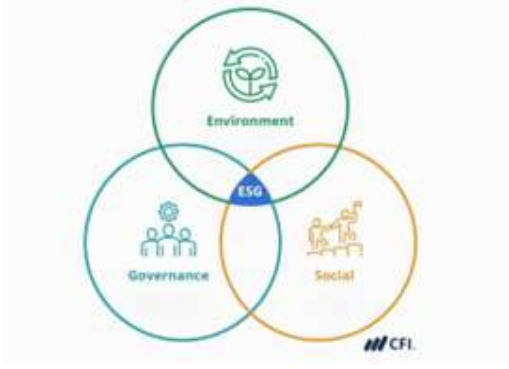


Figure 4: ESG Framework – Environmental, Social & Governance Pillars

Preparing for IPO and Regulatory Scrutiny

Unicorns are working toward their IPO date by

using their internal audit departments to build and be a partner in their strategic transformations. Critical areas of readiness include:

- Design and testing of Internal Financial Controls (IFC)
- Compliance with SOX (or equivalent) for international listings
- Documentation of key processes: P2P, O2C, H2R, and IT General Controls (ITGC)
- Segregation of duties and access governance
- Change management, including controls for system configuration

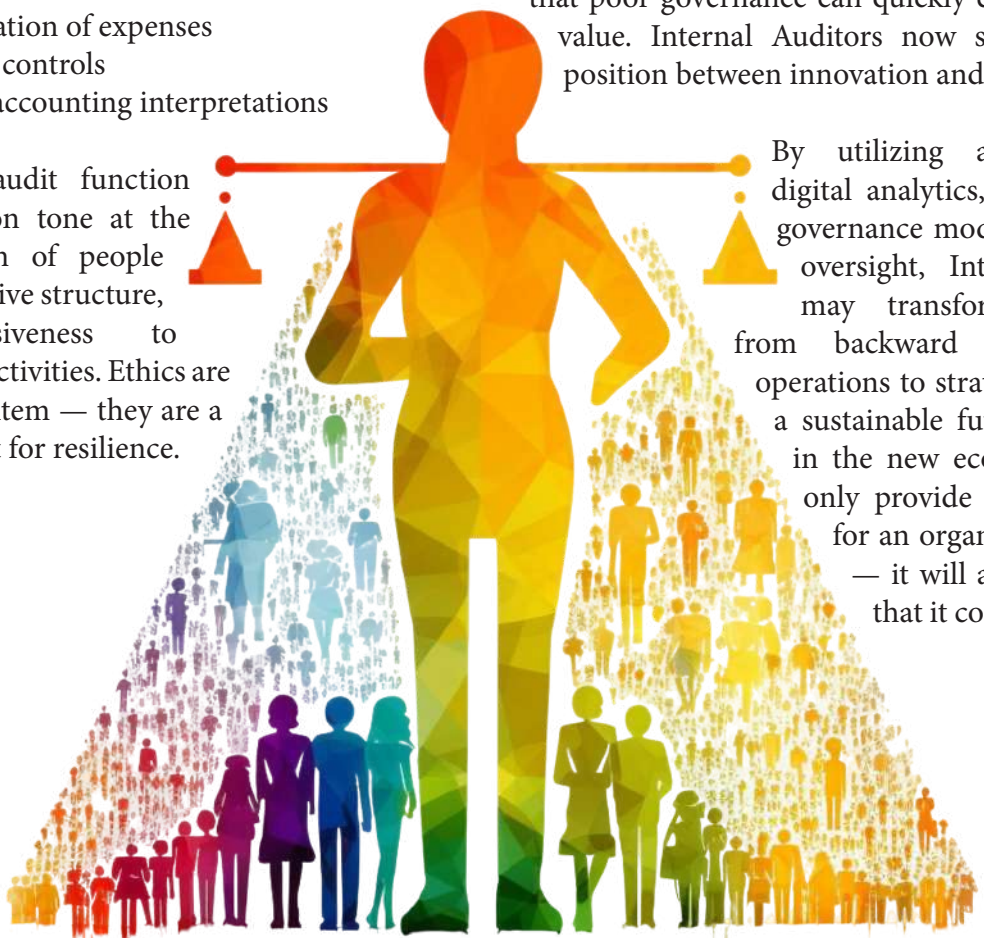
Remediating the issues at the time of IPO is exponentially expensive compared to building out phased maturity. The internal audit function needs to anticipate issues versus be reactive.

The Human Element: Ethics in High-Growth Culture

The root cause of failure for most governance structures is not weak systems; the primary weakness comes from weak ethics culture. The high-pressure growth environment of unicorns can create an incentive to engage in:

- Tactics geared towards revenue acceleration
- Misclassification of expenses
- Override of controls
- Aggressive accounting interpretations

The internal audit function should focus on tone at the top, motivation of people based on incentive structure, and responsiveness to whistleblower activities. Ethics are not a checklist item — they are a multiplier effect for resilience.



The Path Ahead: A Strategic Vision for Internal Auditing

There are five transformative changes needed to audit start-up and unicorn companies effectively:

- **Continuous Assessments:** Replace periodic reviews with ongoing monitoring.
- **Holistic Business Model Review:** Look at the business model as a whole, not just financials.
- **Risk-Based Consultation:** Consult on risk mitigation instead of enforcing compliance.
- **Predictive Analytics:** Use predictive analytics to anticipate risks before they materialise.
- **Scalable Governance:** Develop scalable governance systems rather than fixed ones.

The internal auditor must help ensure innovation is based upon integrity, scalability and trust. In a capital-rich environment, where the market may see a dramatic increase in value overnight, sustainable value is reliant upon maintaining a disciplined approach to governance.

Conclusion

Most startups/unicorns represent ambition, change, and technology. However, past experience indicates that poor governance can quickly erode enterprise value. Internal Auditors now sit in a critical position between innovation and accountability.

By utilizing agile methods, digital analytics, lifecycle-based governance models, and ethical oversight, Internal Auditors may transform themselves from backward evaluators of operations to strategic creators of a sustainable future. Assurance in the new economy will not only provide an opportunity for an organisation to grow — it will also help ensure that it continues to grow.

Auditing the New Economy

Startups, Unicorns & High-Growth Companies

Saakshi Ranka
Scholar – Global Risk Management Institute

The rapid growth of high-growth businesses, unicorns, and startups has completely changed the structure of the global economy. These businesses, which are distinguished by disruptive innovation, asset-light models, digital platforms, and aggressive scaling strategies, pose a threat to established auditing frameworks that were created for stable, asset-heavy organizations. This study looks at how auditing is changing in the "New Economy," emphasizing special risks, complicated governance, uncertain valuations, and regulatory demands. It examines how auditors must adopt risk-based strategies, embrace technology-driven tools, and recalibrate methodologies in order to guarantee accountability, transparency, and stakeholder trust. The study offers a forward-looking audit framework that incorporates environmental, social, and governance (ESG) considerations, cybersecurity risks, revenue recognition complexities, and intangible asset valuation by examining structural differences between traditional businesses and digital-first ventures.

The Nature of the New Economy Enterprise

The business models, funding sources, and risk profiles of startups and unicorns are very different from those of traditional businesses. High-growth businesses typically use asset-light, technology-driven business models, in contrast to established corporations that frequently depend on physical assets and steady revenue streams. Instead of current profitability, their valuations might be based on anticipated future earnings. For example, ride-sharing services like Ola quickly expanded by utilizing digital infrastructure instead of car ownership, radically changing cost structures and operational risks.

The funding environment adds to the complexity of the situation. Large sums of money are injected into early-stage businesses by venture capital and private equity investments, which both accelerate expansion and raise growth expectations. As a result, there is pressure to show performance indicators like market share, revenue growth, and user acquisition. Internal controls, compliance procedures, and financial discipline areas all of which auditors are now required to examine more closely than ever before

can occasionally be overshadowed by the emphasis on speed.

Rethinking the Scope of Audit

Audit functions need to go beyond historical financial verification in the new economy. Financial statements are still significant, but they don't tell the whole story. Non-financial metrics like customer lifetime value, churn rate, burn rate, and gross merchandise value are crucial for high-growth businesses. Compared to traditional profitability metrics, these indicators frequently have a greater impact on investor confidence. As a result, auditors must evaluate the integrity and dependability of operational metrics provided to stakeholders in addition to the accuracy of financial data.

In digital businesses, revenue recognition presents unique difficulties. Accounting treatments are complicated by subscription models, freemium services, bundled services, and multi-sided platforms. A sophisticated grasp of technology-driven business models is necessary to guarantee adherence to accounting standards. Additionally, balance sheets are frequently dominated by intangible assets like algorithms, intellectual property, and brand value. In situations where market conditions can change quickly, auditors must assess impairment risks and valuation techniques.

Governance in Founder-Led Organizations

A small number of executives hold the majority of the decision-making power in many founder-driven startups. Internal governance may be weakened by this structure, even though it can promote speed and innovation. The risk of poor management or financial misstatement is increased in the absence of established board structures, independent oversight, and formalized policies.

Auditors in such environments must assess governance frameworks carefully. This entails assessing the efficacy of audit committees, related-party transactions, disclosures of conflicts of interest, and board independence. Governance standards must match regulatory requirements as businesses grow and get closer to becoming public. An important turning point where audit rigor becomes even more crucial is the move from a private startup to a publicly traded company.

Technology, Data, and Cyber Risk

The core of new economy businesses is technology. Their most valued asset is frequently data. Strong digital infrastructure is essential to operations, including banking systems and e-commerce markets. However, there are hazards to data privacy and cybersecurity associated with this dependency. Financial damages, harm to one's reputation, and legal repercussions might result from violations.

As a result, auditors must incorporate cybersecurity evaluations and IT audits into their purview. It is now crucial to assess incident response procedures, data encryption techniques, access controls, and system resilience. Concerns about ethics and compliance are raised by algorithmic bias and opaque decision-making procedures, which exacerbate the growing usage of artificial intelligence and machine learning. It takes interdisciplinary expertise that combines technology know-how with accounting skills to audit such systems.

Regulatory Complexity and Compliance

The regulatory landscape for high-growth companies is often fluid and fragmented. Fintech companies, for example, have to deal with data protection rules, payment system policies, and banking restrictions. Regulations pertaining to competition and consumer protection apply to e-commerce platforms. In India, oversight organizations like the Reserve Bank of India and the Securities and Exchange Board of India are vital in determining what is expected of financial and listed companies in terms of compliance.

Auditors need to keep up with changing legislation and make sure businesses have sufficient compliance systems in place. Serious repercussions, such as fines, operational limitations, or a decline in investor confidence, may follow failure to comply. Multinational regulatory requirements increase the complexity of cross-border activities and necessitate an audit perspective that is globally educated.

The Challenge of Valuation and Investor Expectations

Unicorns startups valued at over one billion dollars often derive their valuations from private funding rounds rather than public markets. The macroeconomic environment and market mood can cause these valuations to change significantly. The vulnerability of exaggerated expectations has been shown by the recent global recalibration of tech valuations.

In order to guarantee that valuation models are rational and transparent, auditors are essential. This entails examining the underlying assumptions of revenue predictions, similar firm benchmarks, and discounted cash flow assessments. Forecasts that are too optimistic have the potential to mislead investors and skew financial reporting. Professional skepticism becomes especially crucial in high-growth environments to offset entrepreneurial optimism.

Environmental, Social, and Governance (ESG) Considerations

Modern stakeholders increasingly demand accountability beyond financial performance. Even for startups, ESG factors are now a crucial part of company strategy. Concerns about data privacy, the rights of gig workers, the carbon imprint, and the ethical use of AI are becoming more and more important. Concerns around worker classification and benefits, for instance, must be addressed by businesses using platform-based gig models.

It is now expected of auditors to offer assurance about ESG measurements and sustainability reporting. Verifying non-financial facts and evaluating the resilience of sustainability frameworks are necessary for this. A larger move toward comprehensive accountability in the new economy is shown by the incorporation of ESG auditing.

Internal Audit as a Strategic Partner

Internal audit functions are frequently created later in the organizational lifecycle in high-growth businesses. On the other hand, early internal audit integration can yield substantial strategic advantages. Internal auditors can work as risk consultants instead than only enforcing compliance, assisting management in anticipating difficulties related to expanding operations.

Internal audit teams provide long-term resilience through risk assessments, process efficiency evaluations, and control improvement recommendations. Their proactive involvement promotes an accountable culture without inhibiting creativity. In settings where quick iteration and experimentation are crucial to competitive advantage, this balance is crucial.

The Future of Auditing High-Growth Enterprises

Auditing procedures must change as technology advances. Automation, data analytics, and continuous auditing are changing the way audits are carried out. Instead of depending only on sampling methods, auditors can examine complete datasets thanks to sophisticated analytical tools. This enhances accuracy and reduces the risk of oversight.
Moreover, collaboration between financial auditors, IT specialists, data scientists, and legal experts is becoming increasingly necessary. High-growth businesses require interdisciplinary approaches that go beyond conventional accounting knowledge due to their complexity.

Conclusion

In conclusion, agility, technological proficiency, and strategic understanding are necessary for auditing the new economy. Unicorns and startups represent growth and innovation, but they also represent increased risk and uncertainty. Efficient auditing guarantees that fast growth does not jeopardize ethics, governance, or openness. Auditors may protect stakeholder trust and promote sustainable innovation by developing alongside the businesses they assess.

The future of auditing is not just about confirming the past but also about helping businesses expand responsibly and resiliently in a constantly shifting economic environment. The audit profession must continue to be flexible, autonomous, and forward-thinking as the new economy develops.In a time of change, the real test of auditing success will be its capacity to support innovation while maintaining transparency, building resilience, and maintaining stakeholder confidence.

Redefining Internal Audit for the New Economy

From Blitzscaling to Governance

Swagatam Nanda & Amrita Daga

The internal audit (IA) function is undergoing a major transformation as the "New Economy," which is defined by venture-backed startups, unicorns, and high-growth technology enterprises, continues to upend established industries. The "move fast and break things" mentality of blitzscaling frequently conflicts with traditional audit processes, which are designed for steady, physical operations. The change from manual to hyper-automated controls, the distinct risk profiles of unicorns, and how internal auditors may become strategic "agile assurance" partners without losing their independence are all covered in this essay.

Overview: The Paradox of High Growth

Rapid scalability, intangible assets, and often a "growth-at-all-costs" mentality are characteristics of the New Economy. The transition from a garage business to a multinational corporation can occur in months rather than decades for a unicorn (a company worth more than $1 billion). This presents a dilemma for internal auditors: how can they offer solid assurance when the underlying technology, organizational structure, and business model are always changing?

Traditional annual audit plans go out of date in these circumstances before they are even approved. The IA department needs to change from a "policing" approach to an Agile Assurance model that keeps up with business speed and shields the company from serious governance errors in order to remain relevant.

I. Using the Pre-Revenue Audit to Control Pre-Operative Risks

Many high-growth companies operate for years in a pre-revenue or "pre-operative" phase, concentrating on user acquisition and product development. In these businesses, the auditor cannot rely on traditional revenue-cycle analyses or sales-based financial assertions.

A. Cash Runway and Burn Rate Integrity

The biggest risk to a pre-operative firm is mismanagement of investor finances. The auditor must confirm the Burn Rate Integrity to ensure that funds are used in compliance with board-approved directives and are not diverted through unapproved channels. One important metric that auditors should keep an eye on is the Cash Runway:

Runway (Months): Total Cash Balance / Monthly Average Net Burn Rate

The IA function fails in its core responsibility to the Board if it ignores these crucial financial survival measures. A monthly evaluation of burn rate fluctuations and the legitimacy of high-value "customer acquisition costs" (CAC), which sometimes mask internal losses, should be part of audit procedures.

B. P2P Cycle Vendor Management

Startups frequently depend on a few big cloud service providers (AWS, Azure) or specialist marketing firms. The Procure-to-Pay (P2P) lifecycle must be audited in order to prevent fraud. The "Three-Way Match" (Purchase Order, Goods Received Note, and Invoice) is frequently omitted in a high-growth setting in order to save time. IA needs to set up automated notifications for:

Risks associated with Vendor Concentration: Over-reliance on one supplier without a backup strategy.

Hiring "friendly" providers without competitive bidding presents a conflict of interest for founders or early staff.

Payments for SaaS subscriptions that are no longer in use are known as "ghost expenditures," and they frequently cause a hidden drain on startup profits.

II. Dynamic Risk Control Matrix (RCM) and Automated Controls

For a unicorn that handles millions of transactions per day, sample-based manual testing is insufficient. The internal auditor is required to assess and support automated internal controls.

A. Establishing the Current RCM

While a typical RCM is unchangeable, a New Economy RCM must be flexible. High-growth companies' controls should be categorized by auditors based on their "Automation Maturity":

Risk Level	Control Nature	Audit Strategy
High	Difficult Manual choices	Extensive substantial testing and analysis of "Tone at the Top."
Medium	Medium IT Dependency	Analyse the reliability of system-generated reports' (IPE).
Low	Fully Automated	Rely on the setup and "change management" logic after you've tested it once.

B. Identity Governance and Logical Access

User ID breaches pose a serious risk to high-growth companies. The "Least Privilege" principle may suffer as a company expands from 50 to 5,000 employees. Auditors need to verify:

Identity and Access Management (IAM): Do automated scripts generate administrator accounts without leaving an audit trail?

Provisioning/De-provisioning: There is a significant risk of "orphaned accounts" (former employees keeping access) in startup settings with rapid personnel turnover.

III. Entity-Level Governance and the "Founder Effect"

Many unicorns (like WeWork and FTX) failed because of soft control issues rather than IT control issues. The "Founder Effect" can cause a dominant personality to disregard established procedures, which can lead to "Governance Debt."

A. "Tone at the Top" auditing

Internal auditors need to be daring professionals in order to audit the culture. This could involve:

Anonymous Culture Surveys: Finding out if employees feel pressured to "bypass" rules in order to meet growth goals.

Board Reporting Lines: To maintain independence in the face of rapid expansion, the Head of Audit must report directly to the Audit Committee rather than the CEO or Founder.

B. Regulatory Compliance and Basel Frameworks

For fintech unicorns, the stakes are even higher. When a startup becomes a regulated financial institution, strict adherence to capital adequacy criteria is required. Auditors must assess the company's readiness for Basel II/III requirements, specifically:

Risk-Weighted Assets (RWA): Do the automated algorithms accurately determine credit risk?

Tier 1 Capital Ratios: Does the startup have enough liquid, high-quality assets on hand to weather a market downturn?

IV. Putting Agile Data Analytics & Internal Audit into Practice

The IA function needs to use Agile Auditing in order to audit at the speed of a startup. The six-month "Big Bang" audit report is being replaced by two-week "Sprints."

Continuous Auditing (CA): Use Python or SQL to audit "last night," rather than "last year." An auditor might, for instance, create a script that flags any transaction in the ERP system where the "Approver" and "Requestor" share the same User ID.

Predictive Auditing: Usi Identifying potential control failure locations by analysing data trends. The RCM need to automatically alert a department for a "flash audit" if it has a high turnover rate and few training hours.

V. Technical Debt: The Undiscovered Audit Risk

The term "technical debt" refers to the code shortcuts that developers often use in their rush to release products. For an auditor, this means "Control Debt."

A disorganized electronic payment transaction's code increases the risk of cybersecurity problems or erroneous financial reporting.

IA should perform pre-implementation reviews of major system changes (such as SAP integration or a new CRM). By identifying a logic flaw during the "development" phase, the auditor saves the company millions of dollars in potential "remediation" fees after launch.

VI. The Risk of "Shadow IT": Examining Untracked Infrastructure

In businesses that are growing quickly, the pace at which new products are introduced sometimes exceeds the IT department's ability to set up safe infrastructure. This results in "Shadow IT," where employees use third-party APIs, cloud storage, or unapproved SaaS solutions to get around traditional procurement processes. This results in a "blind spot" for an internal auditor where cybersecurity precautions, access controls, and data location are not monitored. In order to audit this, network discovery and SaaS management solutions must replace static asset listings. Every third-party integration must pass a Vendor Risk Assessment (VRA), according to internal audit. This helps ensure that the "quick fixes" of today don't become serious dangers for future data breaches.

VII. Conclusion: Assurance's Future

It takes a combination of traditional professional skepticism and technical data abilities to audit the New Economy. The auditor is now a strategic advisor who makes sure the business "blitzscales" on sound foundations rather than merely a "checker" of boxes. Internal audit's function is to act as the "brakes" that allow startups and unicorns to grow more quickly. Auditors may make sure that high-growth organizations not only scale but also persist by concentrating on automated controls, burn-rate integrity, and agile methodologies.

Sharpen Your Mind: The IA Quiz

Q1. Which risk category most accurately represents the Rs310 crore capitalisation of customer acquisition cost (CAC)?

A. Risk of Liquidity
B. Risk of Earnings Management
C. Risk in Operations
D. Risk to Cybersecurity

Q2. The following are the main effects of outsourcing the internal audit function to an investor-funded company:

A. Objectivity
B. Proficiency
C. Appropriate Professional Care
D. Documentation for Audits

Q3. If three lending partners account for 68% of revenue, the biggest audit concern is:

A. Risk of revenue volatility
B. Risk of supplier concentration
C. Risk of counterparty concentration
D. Risk of regulatory arbitrage

Q4. The increase of the ESOP pool from 8% to 18% without showing profitability suggests potential issues:
A. Risk of dilution
B. Impairment of assets
C. Misstatement of working capital
D. Smoothing of revenue

Section B: Financial Reporting & Accounting Judgement

Q5. Upfront recognition of processing fees on long-term contracts most likely violates which principle?

A. Prudence
B. Matching
C. Revenue Recognition (Ind AS 115 / IFRS 15)
D. Materiality

Q6. The aggressive capitalization of development costs predominantly affects

A. EBITDA inflation
B. Cash flow manipulation
C. Tax evasion
D. Meeting loan covenants

Q7. AI model updates without validation pose risk to:

A. Inventory valuation
B. Expected Credit Loss (ECL) modelling
C. Deferred tax calculation
D. Hedge accounting

Q8. Fair value measurement in loan securitization introduces high exposure to:

A. Level 1 inputs
B. Level 2 inputs
C. Level 3 inputs
D. Historical cost distortion

Section C: Internal Controls & IT Risk

Q9. A weak segregation of duties in data analytics could MOST directly lead to:

A. Data exfiltration
B. Management overriding controls
C. Risks of model manipulation
D. Payroll fraud

Q10. A high attrition rate of 35% in risk and compliance leads to:

A. Detection Risk
B. Inherent Risk
C. Control Risk
D. Sampling Risk

Section D: Strategic & Emerging Risks

Q11. What does the unicorn's valuation, despite a Rs420 crore loss, most clearly indicate about the audit focus?

A. Impairment of goodwill
B. Going concern assumption
C. IPO readiness controls
D. ESG reporting reliability

Q12. When it comes to using alternative data like UPI and social signals, what new audit risk emerges?

A. Climate risk
B. Privacy & Data Protection compliance
C. Inventory obsolescence
D. Foreign exchange exposure

Q13. If GNPA is reported at 2.1% but ECL coverage is only 18%, what should the auditor be most concerned about?
A. Under-provisioning risk
B. Cash flow misclassification
C. Off-balance sheet financing
D. ESG misreporting

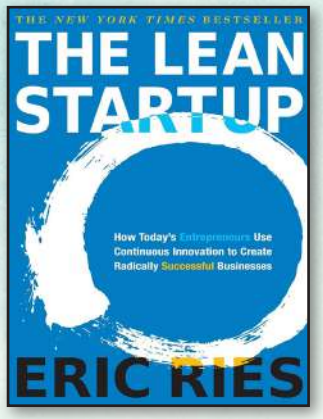
Section E: Bonus – Advanced Audit Scenario

Q14. If FinNova is gearing up for an IPO in 12 months, which of the following becomes essential?

A. SOX-like internal control documentation
B. Cyber maturity assessment
C. Revenue contract standardization
D. All of the above

BOOKS THAT MATTER

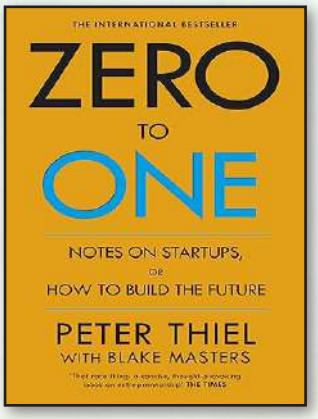
Top Picks for IA Professionals



The Lean Startup — by Eric Ries
Why it fits your theme:
This is foundational for understanding how startups operate—rapid experimentation, MVPs, and pivoting.
Relevance for Auditors:

- Helps understand non-traditional business models
- Insight into risk-taking vs. control environments
- Useful to audit innovation-driven processes

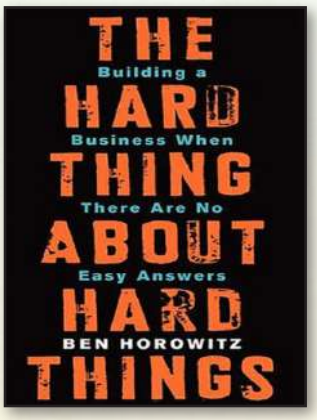
Best takeaway:
Startups prioritize learning over perfection—controls must adapt to this mindset.



Zero to One — by Peter Thiel
Why it fits:
Focuses on building unique, monopoly-like businesses—exactly what unicorns aim for.
Relevance for Auditors:

- Understanding scalability risks
- Evaluating founder-driven decision-making
- Insight into long-term vs short-term value creation

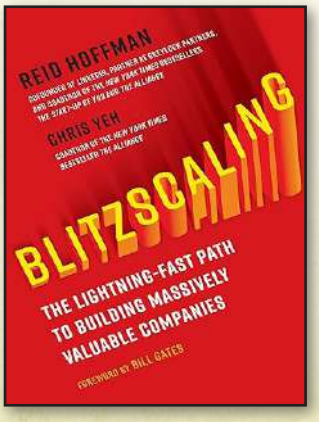
Best takeaway:
Great companies don't just compete—they create entirely new markets.



The Hard Thing About Hard Things — by Ben Horowitz
Why it fits:
Gives a real, unfiltered look at challenges in scaling companies.
Relevance for Auditors:

- Understanding crisis management and governance gaps
- Real-world view of people, culture, and controls
- Helps assess leadership risks

Best takeaway:
There are no textbook solutions in high-growth companies—judgment matters.

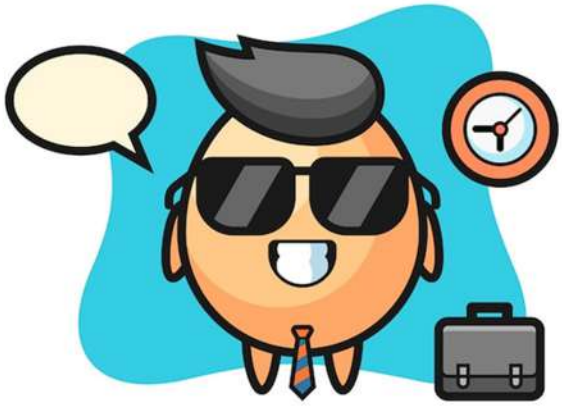


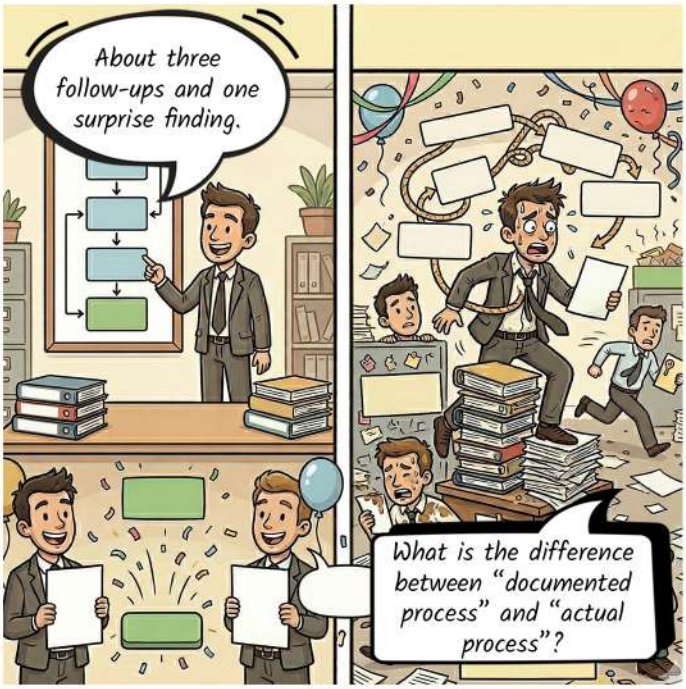
Blitzscaling — by Reid Hoffman
Why it fits:
Perfectly aligned with unicorns and hyper-growth companies.
Relevance for Auditors:

- Explains speed vs control trade-offs
- Helps identify risks of scaling too fast
- Useful for auditing process maturity gaps

Best takeaway:
In hypergrowth, companies often accept inefficiencies—auditors must identify when it becomes a risk.

Humour in Action





AROUND THE WORLD AUDIT INTELLIGENCE FROM ACROSS THE WORLD

Playing the Long Game

Auditing the organization's strategy, piece by piece, can help ensure the business achieves its vision.

Eric Wilson Rheya Tanner

One of the most memorable moments early in my career came when an audit committee chair tasked me with auditing the company's corporate strategy. Although I was excited about working on this high-profile project, I struggled with how to approach the daunting task.

Questions swirled: How could my team audit something as broad as strategy? If the audit uncovered a major flaw, would leadership rethink its entire strategic plan? How would internal audit navigate the sensitivities of challenging senior management's vision for the company?

But first, I had to grapple with a greater question: After more than a decade in internal audit, why was this the first time my function had audited organizational strategy?

Auditing an organization's strategy is a critical yet often overlooked responsibility for internal audit functions. Strategic risks are among the top threats today's organizations face, outpacing operational, legal, compliance, and financial risks. According to PwC's 2023 Global Internal Audit Study, 68% of leaders seek internal audit's input on strategy, yet only 34% of audit efforts target these risks.

By auditing strategy, internal audit can help ensure strategic plans are aligned with market realities, safeguarding long-term competitiveness. This approach can strengthen governance and position internal audit as a strategic partner to the board and management.

However, many internal audit teams shy away from strategy reviews for several reasons. First, auditors may feel they lack expertise in auditing broad, ambiguous strategic plans. Second, many organizations see internal audit as a tactical function rather than a strategic one. Finally, some audit functions still consider legal and financial risks to be paramount despite data showing that strategic risks drive greater losses. Overcoming these barriers is crucial for internal audit to deliver value where it matters most.

One Move at a Time

There is an old saying: "How do you eat an elephant? One bite at a time!" Although strategy audits can feel akin to balancing a nation's budget overnight, they often unfold over multiple projects and span a year or more. That way, auditors can address an organization's strategic risks piece by piece — a process auditors are accustomed to with limited resources and broad organizational mandates.

Enter internal audit's trusty tool: the risk assessment. Risk assessments help auditors prioritize the components of strategy audits, giving both practitioners and management a useful guide to review key topics. Including strategic risks in these assessments can highlight areas that need attention and provide auditors with data to justify allocating time and resources to them. Over time, the list of strategic risks may grow, but auditors should begin by considering several key attributes.

Risk Appetite Definition. Internal audit should assess whether the organization's risk tolerance aligns with its strategic goals. Auditors should evaluate what leadership defines as acceptable risk levels for major initiatives.

Stakeholder Engagement. Internal auditors should review the input provided by executives, board members, and external advisors in the strategy-setting process. They should check whether there is clear documentation showing that different opinions were shared and considered. Auditors also should evaluate whether various groups are aligned with the strategy. For example, if the board considers one area of the strategy to be particularly risky but the CEO mentions another area of risk, performing a communications and performance measurement audit could identify how to align these views.

Organizational Alignment. As internal audit completes risk surveys and interviews, it should assess whether the organization's various disciplines and functions are aligned with the overall strategy. Are there disconnects that may be driving the organization to misallocate resources or fail to fully realize its strategic goals?

Strategic Content Assessment. Internal audit should assess the assumptions and risks management considers when it sets the organization's strategy. What time frame do market projections cover and are they realistic? What forms of competitive analyses, financial models, and external data, such as industry reports, does management use to support the strategy?

Scenario Planning. Internal audit should check whether management has processes in place to stress-test strategies against risks. Auditors should assess whether the scenario models are sufficiently robust, considering the organization's industry, operating locations, and competitive landscape.

Strategic Risk Identification. Auditors should verify whether management has developed methods to pinpoint top risks, such as cybersecurity, digital transformation, and the impact of political actions. Do risk registers provide comprehensive coverage?

Prioritization Framework. Internal audit should examine how management ranks


As the CEO and I stared at each other — me, the data-driven auditor, and him, a visionary strategist — I felt out of my depth.
Internal Auditor
49

and prioritizes strategic risks. Are the weighting criteria complete and aligned with the risks' potential business impact? Can management clearly articulate a framework? If not, auditors may consider performing a basic audit of management's strategy-setting and implementation processes.

Embedding these components into internal audit's risk assessment can turn a mountain of risks into manageable bites. This risk-based approach also can help audit functions plan audits that align with the organization's strategic vision. Moreover, it enables internal audit to advocate for using best practices in organizational strategy and identify gaps that can be tracked and measured during each assessment cycle.

A Metrics-Driven Plan

When I began planning my first strategy audit, one of my first stops was the CEO's office. When I asked him how he shaped the company's successful strategy, he shrugged and said, "I have no idea."

The CEO genuinely couldn't articulate the data, reports, or metrics that guided his vision. "It's a gut feeling," he explained, citing his industry experience and his circle of trusted advisors and key resources. He said he deferred to his instincts in setting a strategy that would guide how the company would drive and allocate billions of dollars in revenue and expenses. In short, the company's success hinged on what seemed to be a hunch.

This CEO's approach, while successful, isn't always how executives and boards set strategy. In fact, it is typically the opposite. However, auditors must be prepared to evaluate strategy in organizations, no matter what approach is used to develop it.

As the CEO and I stared at each other, I felt out of my depth. Yet working together, we crafted a plan. It quickly became apparent that even in intuition-driven organizations, the audit function can successfully assess key aspects of organizational strategy.

During that first audit, the CEO and I agreed to review metrics-driven items that established internal audit's ability to evaluate the organization's strategy. This approach not only helps validate an organization's strategy but also sets the stage for planning long-term audits through risk assessments.

Review and Approval. Internal audit should assess the process management uses to develop its strategy. Are the board's reviews of the process thorough, with documented inputs and outputs? Auditors should check meeting minutes for evidence that the board challenged the strategy before approving it.

Internal audit also should benchmark board reviews against various frameworks. Do ongoing strategy sessions include external risk data? How involved are independent directors in those sessions?

Communication Process. Internal audit should evaluate how management communicates its strategy throughout the organization. Do executives clearly articulate the strategy in town halls or memos? Auditors should assess whether employees understand the strategic vision by conducting surveys, interviews, and reviews of department plans and budgets.

Success Metrics. Internal auditors should examine how well the organization defines its success metrics, such as market-share growth, free cash flow, and net-promoter scores. Are key performance indicators (KPIs) specific, measurable, actionable, realistic, and time-bound? Are they tied to the organization's strategy?

Measurement and Reporting. Internal audit should determine how frequently the organization tracks metrics and reports them to leadership. Are reports timely and actionable? At what level of detail is the board apprised of results?

Resulting Actions. Auditors should analyze responses to metric outcomes. Do underperforming metrics trigger strategic changes such as a reallocation of resources? Are there trigger points in the KPIs that would require management to reevaluate the organization's strategy? Practitioners should audit management's action plans for follow-through.

Positioned to Advise

Internal audit shouldn't wait until the organization's strategy is in place to provide assurance and advice. Identifying issues and improvement opportunities after a strategy is rolled out is akin to questioning a roller coaster's safety after the train has left the gate — at that point, you are just along for the ride.

Fortunately, the Global Internal Audit Standards provides guidance on performing advisory services. By following the Standards, practitioners can lead from the front, helping the organization design systems and processes associated with the strategy before it is in place.

Of course, auditors still cannot own decisions and outcomes. However, by providing feedback while the strategy is being developed, internal audit can help identify problems before they happen. This reduces risks for the

organization and enhances internal audit's value.

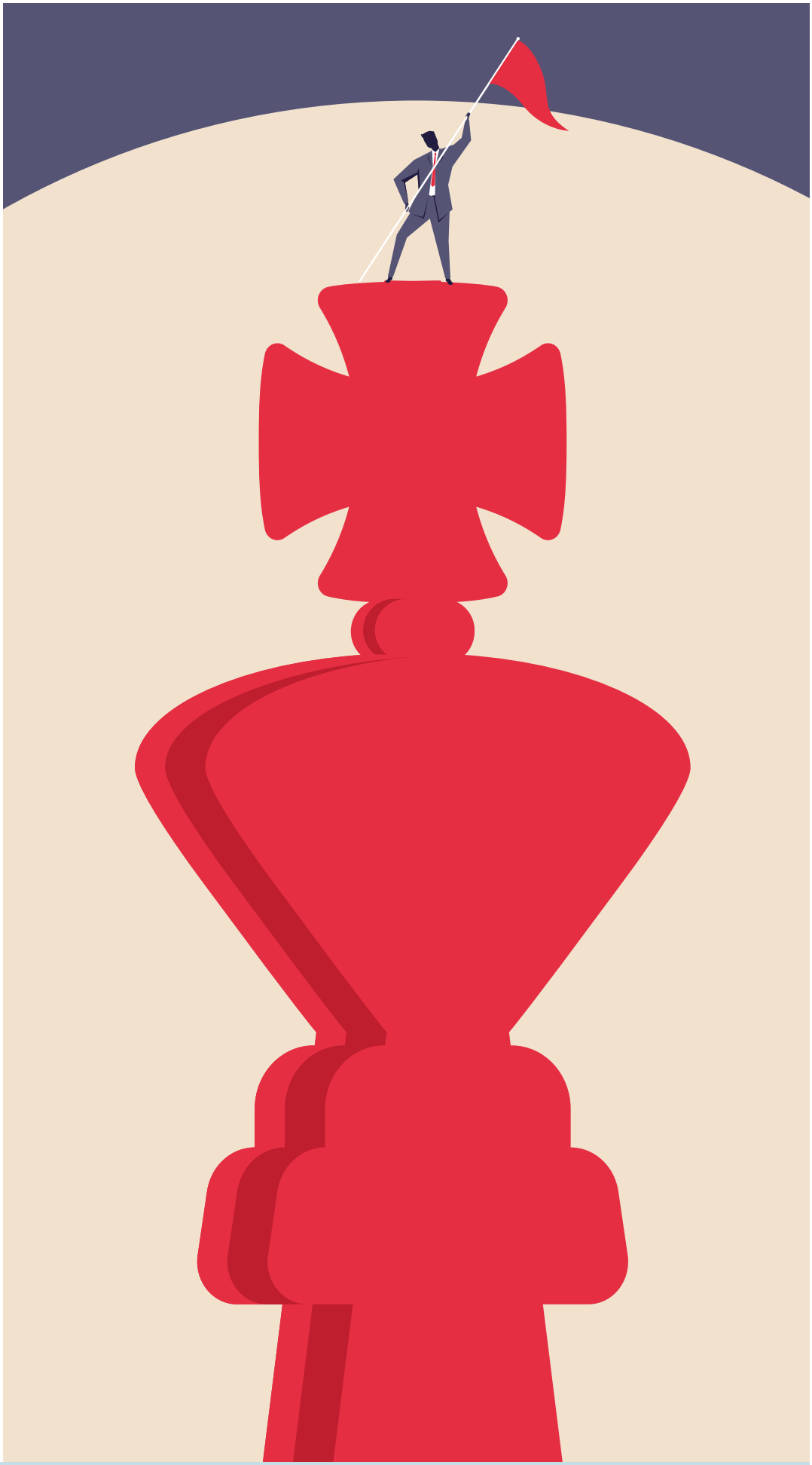
Before internal audit can start taking on consulting projects, it needs to complete a few administrative steps. It must update the audit charter and ensure management agrees that auditors should perform consulting work. Although it may take some extra effort, it's worth it — especially when consulting on strategy enables internal audit to better support management's goals.

The Next Move

Auditing an organization's strategy is critical, as strategic risks consistently outrank all other risks. Internal auditors can help executives turn their "gut" vision into clear decisions based on data from structured reviews of strategy, goals, and internal audit's support in the development and deployment of strategic goals.

Internal audit shouldn't let barriers such as expertise gaps or administrative hurdles stop it from reviewing the organization's strategy. Instead, it should address strategic risks with the clarity used in any other audit. This approach will enable the function to deliver value, align audits with business needs, and contribute to the organization's success.

Eric Wilson, CIA, is director, Internal Audit, and CAE at Gulfport Energy in Oklahoma City.



This article was originally published digitally by "IIA Global" in Aug 2025. It has been republished here for our readers who can access the publication on https://internalauditor.theiia.org/en/articles/2026/Apr

Joining The IIA is an investment in your career and the profession.

Bengaluru	8022261371	bangalorechapter@iiaindia.co
Chennai	9884716160	madraschapter@iiaindia.co
Delhi	9650002331	delhichapter@iiaindia.co
Hyderabad	9391690256	hyderabadchapter@iiaindia.co
Kolkata	7980586848	calcuttachapter@iiaindia.co
Mumbai	9326652393	bombaychapter@iiaindia.co
IIA India	8287359493 9004512247	Coordination@iiaindia.co Coordinator@iiaindia.co

The Institute of
Internal Auditors
India

JOIN US ON SOCIAL MEDIA

LASER

DON'T JUST MEET THE STANDARDS, SET THEM WITH LASER.

Your Trusted Partner in Proactive GRC & Audit Management

BUILT FOR BUSINESSES THAT LEAD, NOT JUST COMPLY.

TATA · ADITYA BIRLA GROUP · BAJAJ · JSW · Godrej

THE LASER SUITE

- LASER Audit Reporting System
- LASER Enterprise Risk Management System
- LASER Legal Compliance System
- LASER Internal Controls Manager

INTRODUCING LARS

Automating the Complete Internal Audit Lifecycle

- End-to-end audit automation
- Real-time dashboards and customizable reports
- Risk-Based Internal Audits as per RBI Guidelines
- Automated Workflows & Checklists

THE LASER EFFECT

Key Impact Metrics

90% Faster Audit review & resolution	**95%** Improvement in Risk understanding & management
80% Reduction in non-compliance occurrences	**100%** Enhancement in Internal Controls efficiency

EXPERIENCE THE LASER ADVANTAGE. BOOK A DEMO TODAY!

9833660742 · enquiry@lasergrc.com · lasergrc.com

This magazine is digitally published by the Institute of Internal Auditors, India.
Reach us at: publications@iiaindia.co