www.iiaindia.co

Volume-32 | June 2026 Edition

Internal Audit Today

INTERNAL AUDIT REIMAGINED

Redefining Internal Audit in the age of AI

The Institute of Internal Auditors India

Table of CONTENTS

EDITORIAL

EXPERT VOICES - LEADERSHIP SERIES

THE INSIGHT EXCHANGE - AUTHOR'S CONVOS

Table of CONTENTS

EMERGING MINDS – STUDENTS' FORUM

AROUND THE WORLD

IIA INDIA HAPPENINGS

Chairperson's Communique

Reimagining Assurance. Inspiring Impact. Shaping the Future.

Dear Readers,

It gives me immense pleasure to present the June edition of IA Today, centered around the thought-provoking theme, "Internal Audit Reimagined."

The profession of internal audit is evolving at an unprecedented pace. Today, internal auditors are not only assurance providers but also strategic partners who enable resilience, governance, innovation, and sustainable growth. As businesses navigate technological disruption, regulatory changes, cyber risks, ESG expectations, and dynamic stakeholder demands, the role of internal audit continues to expand beyond traditional boundaries.

This edition captures that transformation through diverse perspectives, practical insights, and future-focused discussions contributed by leaders and professionals across industries.

The month of May also held special significance as we celebrated Internal Audit Awareness Month. It was inspiring to witness enthusiastic participation from chapters across the country through knowledge sessions, outreach initiatives and social media campaigns aimed at strengthening awareness about the value and impact of the internal audit profession. These collective efforts reaffirmed the growing recognition of internal audit as a catalyst for trust, transparency, and organizational excellence.

I extend my heartfelt gratitude to all contributors, authors, reviewers, chapter leaders, volunteers, and members of the internal audit community whose dedication and thought leadership have made this edition possible. Your commitment towards knowledge sharing and professional excellence continues to strengthen our fraternity and inspire the next generation of auditors.

As we move forward, let us continue to reimagine internal audit , not merely as a function of compliance, but as a profession that drives insight, foresight, and meaningful impact. The future belongs to professionals who remain adaptable, collaborative, and committed to continuous learning.

I hope this edition of IA Today provides valuable perspectives and encourages enriching conversations within the profession.
Happy Reading!

warm regards,

Pooja Dharewa

Chairperson
IIA India Publication Committee
pooja@kdpractice.com

President Communique

Internal Audit Reimagined: Touchless Assurance, Human Insight, and the Courage to Care

Internal audit is at the edge of reinvention.

Technology is moving at a pace few professions can ignore. Automation, analytics, artificial intelligence, and real-time monitoring are changing how assurance is designed, delivered, and consumed. The question before us is no longer whether audit will change, but **how boldly we are willing to reimagine it.**

Can a significant part of internal audit become touchless?

Increasingly, yes.

Routine controls, exception monitoring, transactional testing, and data-led assurance can move closer to process owners who live with the data. Technology can create continuous visibility into what is working, what is failing, and where risk signals are emerging. Internal audit, in such a model, does not disappear. **It rises.**

If touchless assurance gives us the signals, internal audit must bring interpretation. If automation tells us what has gone wrong, auditors must help the organisation understand why it matters, what it reveals, and how the control environment can mature.

This is where the profession must move from testing controls to **strengthening control consciousness.**

The future audit function will not sit outside the business as a distant reviewer. It will work with teams to imagine better controls, smarter monitoring, and how risks can be anticipated before they become findings. That partnership requires maturity, trust, and the belief that assurance enables better business.

Yet, even as technology accelerates, we must ask an uncomfortable question.

Where is the human quotient in audit?

Audit programs, risk control matrices, workpapers, reports, dashboards, and systems are important. They give discipline to the profession. But they cannot replace conversation.

Audits are built through conversations.

The most meaningful insights emerge not at the desk, but

in dialogue. They emerge when auditors walk the floor, speak informally with teams, understand pressures, listen without judgment, and create trust for people to share what documentation may never reveal.

Too often, auditors are criticised for having a narrow view, for not joining the dots, or for not appreciating business realities. That criticism must be heard with humility.

The answer is not to reduce independence. It is to **deepen understanding.**

Auditors must become more curious about the business, more alive to its context, and more willing to engage beyond formal touchpoints. Only then can they connect risk, controls, operations, culture, and strategy into a holistic view.

Internal audit also needs empathy.

Empathy does not weaken objectivity. It **strengthens relevance.** It asks whether we truly care for the people we audit, handhold when needed, challenge when required, and allow teams the space to own their responsibilities while knowing that audit stands as a partner in improvement. The reimagined auditor is both technological and human.

Comfortable with touchless assurance, yet committed to meaningful conversation. Skilled in analytics, yet grounded in empathy. Independent in judgment, yet collaborative in spirit.
In that balance lies the future of internal audit.

Not less human because of technology, but more human because technology gives us the space to rise into **insight, stewardship, and trust.**

With warm regards,

Krishnan Venugopal

President, IIA India

Chief Editor

Dear Esteemed Members and Readers,

We stand at a pivotal moment: artificial intelligence is reshaping how organizations operate, decide, and create value. This June edition, Internal Audit Reimagined, explores how AI transforms risk, control, and assurance—and how internal auditors must adapt from traditional guardians to intelligent enablers of trustworthy innovation.

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.

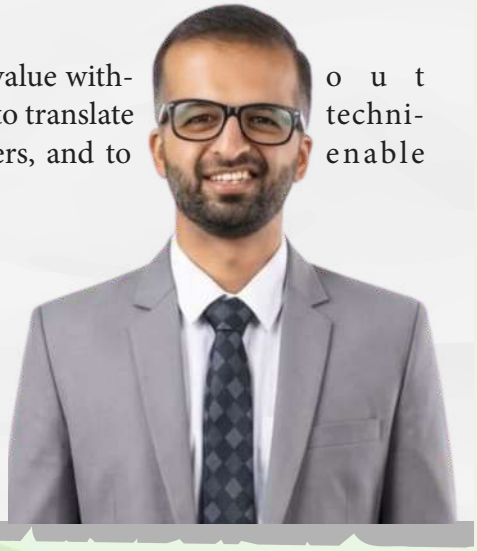
AI brings extraordinary opportunity: faster anomaly detection, continuous auditing, predictive risk insights, and automation that frees auditors for higher-value judgment work. Yet it also introduces new vulnerabilities—model bias, data governance gaps, opaque decisioning, and third-party AI supply-chain risks. Our role is to ensure that AI's promise is realized responsibly, ethically, and transparently.

From Assurance to Augmentation

Auditors must learn to partner with AI—using it to augment professional scepticism, not replace it. That means building fluency in data science concepts, validating model performance, testing training data integrity, and assessing governance around AI lifecycle management. It also means reframing audit methodologies to include continuous monitoring, scenario testing for algorithmic outcomes, and controls that span data, models, and human oversight.

This issue helps you operationalize AI assurance—offer a practical, action-focused roadmap for auditors navigating AI: they translate technical concepts into governance-ready controls, show how to test outcomes and manage bias at scale, outline lifecycle practices for model validation and monitoring, clarify how to explain AI risks to boards in plain governance terms, and provide sector-specific checklists and maturity milestones you can apply immediately—so you can prioritize quick wins, design phased pilots, and turn technical findings into board-level assurance

The mission before us is clear: to ensure that AI accelerates value without compromising trust. As auditors, we are uniquely positioned to translate technical complexity into reliable assurance, to protect stakeholders, and to enable innovation that endures.



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

Arjun Golar
Deputy Editor
arjun.golar@protivitiglobal.in

Arun Kasat
Quality Reviewer
kasatarun@gmail.com

Chanchal Mishra
Lead Co-ordinator
coordination@iiaindia.co

Sandeep Singh
Design Head
sandeep@letsdigitalmarketing.com

PUBLICATION COMMITTEE

Karthik Varadharajan
Member
vksuccess777@outlook.com

Amit Sharma
Member
amitsharma5@hotmail.com

Anand Gupta
Member
anandguptain@gmail.com

Our Contributors

Amit Sharma

In "Agentic Audit: Transitioning from Automated Testing to Autonomous AI Audit Workflows," Amit Sharma explains how auditing is evolving from rule-based automation to autonomous AI agents. These systems enable continuous monitoring, adaptive learning, and deeper risk insights. While efficiency improves significantly, challenges like governance and trust remain. He emphasises that human auditors will continue to provide critical oversight, judgement, and ethical direction.

Flip to Page 28

Rahul Mishra

In "The Ethical Auditor in the Age of Artificial Intelligence," Rahul Mishra highlights how AI-driven decisions introduce ethical risks such as bias and lack of accountability. He argues that auditors must go beyond compliance to assess fairness, transparency, and outcomes. The article positions auditors as key guardians of ethical integrity in organisations increasingly dependent on algorithmic decision-making.

Flip to Page 32

Swapnil N. Mithapelli

In "Auditing AI Algorithms: Governance, Bias, and Accountability in AI Models," Swapnil Mithapelli discusses the need for strong AI governance across the lifecycle. He focuses on fairness, transparency, and accountability while addressing bias and "black box" challenges. The article underscores continuous auditing and structured frameworks to ensure AI systems align with regulatory, ethical, and organisational goals.

Flip to Page 38

Rajat Mohan

In "Board Expectations Reset: How Audit Committees View AI-Enabled Assurance Functions," Rajat Mohan explains how AI is redefining board expectations. Audit committees now prioritise trust, transparency, and clear explanations of AI outputs. The article highlights that while AI enhances efficiency, human judgement remains essential to interpret insights and strengthen governance communication.

Flip to Page 44

Aditya Kumar S.

In "Audit of AI vs. AI in Audit," Aditya Kumar S. distinguishes between auditing AI systems and using AI in auditing. He explains that both require different skills and governance. Addressing risks like automation bias and shadow AI, the article emphasises balancing innovation with professional scepticism and ethical responsibility.

Flip to Page 47

Amita Kavle

In "Strengthening Digital Trust: The Expanding Role of Internal Auditors in Digital Data Protection," CA Amita Kavle explores the impact of India's DPDP Act, 2023. She outlines how auditors must assess privacy risks, consent, and data governance, especially in BFSI. The article positions internal auditors as key players in ensuring compliance and strengthening digital trust.

Flip to Page 58

Manish Tibrewal

In "Reimagining Audit Methodology in a Full-Population Testing World," Manish Tibrewal explores the shift from sampling to full-population testing using data analytics. He highlights how auditors must interpret insights, identify risks, and manage data overload. The article positions continuous auditing as key to delivering timely, forward-looking assurance.

Flip to Page 66

The Institute of Internal Auditors India

EVENT SCHEDULE

JUNE & JULY 2026

01 JUNE

WEBIN R

04:00PM - 05:00PM

W RENESS SESSION ON CI CH LLENGES & 3 P RT EX M*

05 JUNE

T J S NT CRUZ, MUMB I

09:00 M - 06:00PM

6TH NNU L BFSI CONC L VE

06 JUNE

WEBIN R

03:00PM - 05:00PM

UDIT OF NEW- GE & ST RT UP BUSINESSES

18 JUNE

WEBIN R

02:00PM - 06:00PM

ONLINE TR INING ON GLOB L TR INING MODULE-FUND MENT LS OF INTERN L UDITING

19&20 JUNE

NNU L CONFERENCE

09:00 M to 05:30PM

UDIT REM GINED: INTELLIGENCE - INTEGRITY - IMP CT

23 JUNE

WEBIN R

02:00PM - 06:00PM

ONLINE TR INING ON GLOB L TR INING MODULE-FR UD UDITING

27 JUNE

WEBIN R

03:00PM - 05:00PM

UDITING THE PROCUREMENT & SUPPLY CH IN FUNCTION

08 JULY

WEBIN R

02:00PM - 06:00PM

ONLINE TR INING ON GLOB L TR INING MODULE-DEVELOPING UDIT FINDINGS

22 JULY

WEBIN R

02:00PM - 06:00PM

ONLINE TR INING ON GLOB L TR INING MODULE-HIGH IMP CT UDIT REPORTING

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

The Institute of Internal Auditors India

professional excellence, and the pursuit of the highest standards in governance, risk management, and internal audit.

Ch ee

Over the years, I have met many bright students and young professionals eager to pursue the CIA journey – individuals with the talent, discipline, and aspiration to excel in the profession. The thought behind the IIA India CIA Scholarship initiative was simple: to encourage such individuals at an important stage of their professional journey and give them that extra push of confidence and support.

In many ways, I see this much like sport. Talent is important, but talent alone is rarely enough. Every athlete benefits from encouragement, coaching, opportunities, and someone who believes in their potential early in the journey. Professional careers are no different. Sometimes, a small nudge at the right time can make a meaningful difference over the long term.

This initiative is therefore not merely about financial assistance. It is about recognizing merit, rewarding commitment, and encouraging more professionals to invest in themselves and their future. It reflects IIA India's belief that the profession grows stronger when capable and motivated individuals are encouraged to pursue excellence.

Importantly, this initiative has only been possible because of the strong foundation built by the many Past Presidents, National Councils, CEOs, and office bearers of IIA India over the years. Their stewardship and commitment have helped build an institution that is today able to meaningfully invest back into the future of the profession.

Reading through the reflections of our first 20 scholarship recipients has been deeply encouraging. I congratulate each of them on taking this important step in their professional journey. Their sincerity, ambition, and passion for learning reaffirm why initiatives like this matter – and why we are committed to growing it.

This marks the beginning of what should become a flagship long-term initiative of IIA India – one that supports, encourages, and inspires generations of future CIA professionals while further strengthening the internal audit profession in India.

Burzin

Burzin Dubash
Past President - IIA India
Chair - IIA India Scholarship Committee

Congratulations to the First 20 CIA Students Receiving the IIA India Scholarship! A proud milestone for IIA India as the first 20 CIA students receive the IIA India Scholarship to pursue the globally recognized Certified Internal Auditor (CIA) qualification. This initiative reflects IIA India's commitment to nurturing future internal audit professionals and encouraging students and young professionals to build careers in internal audit, governance, risk management, and compliance.

My learning experience has been excellent, and I'm motivated to become a CIA because of the value it brings to companies and society. This inspired me to pass Part 1, and now I am focused on clearing Part 3; an IIA scholarship would support me financially and motivate me to complete all three parts as soon as possible.

I am very much honored to have received the scholarship for CIA. This support provides great encouragement, bringing me closer to my professional goals. Thank you!

I would like to sincerely thank the Institute of Internal Auditors India for providing me with the opportunity to be considered for the scholarship selection. I am truly grateful for this recognition and for the platform that encourages aspiring internal audit professionals like me to grow and excel. As a fresher, this opportunity is extremely valuable as it not only offers financial support but also boosts confidence and provides recognition at an early stage of my career.

Thank you for providing me this scholarship as it will be helpful for me cause I don't come from a well settled background and this help from your side will be a great help to me.

I would like to sincerely thank you for selecting me for the Scholarship. I am truly grateful for this opportunity and honored to be chosen.

A fantastic initiative by [redacted]. This scholarship [redacted] is instrumental in helping dedicated professionals overcome financial hurdles, allowing them to pursue their CIA certification without delay.

I am writing to express my sincere gratitude to the Institute of Internal Auditors India for awarding me the scholarship. I feel truly honored to have been selected. This scholarship is not only a financial support but also a great source of motivation for me to continue striving for excellence in my academic and professional journey in the field of internal auditing. It has strengthened my commitment to work harder and contribute meaningfully to the profession. I deeply appreciate the trust and confidence you have placed in me. I will make the most of this opportunity and uphold the values associated with this prestigious recognition
Thank you once again for your generous support.

Thank you so much for the update regarding the CIA scholarship status. I am grateful to the Institute for this opportunity. At this stage in my professional journey, while I am not working and focused on full-time study, this financial support is incredibly meaningful. It will really help me stay dedicated to my goal of becoming a Certified Internal Auditor very soon.

Thank you for maintaining a program that recognizes and supports students in their time of need. I truly hope this initiative continues for years to come, as it provides a vital lifeline for many aspiring professionals.

The I
Inter
India

"Im truly grateful to IIA India s scholarship. It's an incredible t empowers aspiring professionals like me to pursue globally recognised opportunities in internal audit.

I would like to express my sincere providing a scholarship to a needy truly appreciate your been a great help in offering a strong handhold during a phase of career disparity caused by limited financial resources.
Your support has not only eased my financial burden but has also motivated me to stay focused on building my career with confidence and determination. It has given me hope and encouragement to move forward and strive for better opportunities.
Thank you once again to the IIA India and entire scholarship scrutiny team for your kindness and support

I am grateful to have been sho the IIA Scholarship. This opportu a lot to me, as it will help me balance my CIA studies with better focus and less financial stress.
I am passionate about Internal Audit and eager to learn and grow in this field. This support will motivate me to work harder and achieve my goals. not for me, those who are pursuing also will get a better motivation by this initiative. This will help a lot of people also. Great initiative by IIA India.

I am writing this to gratitude for being sho the IIA scholarship. I sincerely appreciate the opportunity.

I have been informed that my applicatio selected for the scholarship upon exams. Upon receiving this award, express my sincere gratitude for choosing me as a recipient of the IIA India - CIA Scholarship.
I am currently working in an audit firm (S Viswanathan LLP) as an Audit Assistant. The financial assistance has significantly eased my financial burden and will get me one step closer to my academic and career goals. I am really excited to start my journey in Internal Audit.
Thank you again for this opportunity. I am committed to making the most of this scholarship and contributing positively to the field of Internal Audit.

I am sincerely honored to have been selected scholarship program for the Certified Internal (CIA) examination by the Institute of Internal India (IIA India). Being from an economically disadvantaged background, this support is of immense significance to me. This scholarship not only alleviates financial constraints but also strengthens my commitment to pursuing professional excellence in the field of internal auditing. I am deeply appreciative of IIA India's initiative in recognizing merit and providing opportunities to deserving candidates. I extend my heartfelt gratitude for this support, which will enable me to progress toward my academic and professional aspirations with greater confidence and determination.

I'm thankful to IIA India for the schol program. The scholarship will help support me to attempt tge exams. Thanks IIA India!

I am sincerely grateful for being nominated IIA India Scholarship. I am determined to my CIA certification this year and career in internal audit. This scholarship will significantly support my journey and help me stay consistent in my efforts.

The IIA Scholarship Program is opportunity for internal auditors financial support to help pass certification.
It offers reimbursement of exam fees to meritorious and eligible candidates.
This enables professionals to enhance their skills and knowledge without financial burden.
The initiative accelerates career growth and promotes excellence in the field of internal auditing

I am deeply honored and grateful selected for the IIA scholarship in journey. This recognition and strengthens my commitment to pursuing excellence in the field of internal auditing. As a student currently pursuing my MBA, this scholarship comes at the most meaningful time — reinforcing my academic journey and fueling my ambition to grow as an internal audit professional. This scholarship is not just financial support; it is a vote of confidence that I will carry with me every step of the way."

I liked the scholarship scheme helped me for my exam fees Thanks for students from middle class family

I would like to thank you for awarding for CIA exam. I truly appreciate your encouragement, which motivates me striving for excellence in the internal audit profession

FOR MORE DETAILS 8287359493 coordination@iiaindia.co

THE CONTROL ROOM

INDIA'S GLOBAL INTERNAL AUDIT COMMUNITY | LASER GRC

From Inside-Out to Outside-In: The Internal Auditor of Tomorrow

Nagesh Pinge

Past Chair, IIA-India
Audit Committee Chair, Multiple Boards
nagesh.pinge@gmail.com

My association with Laser GRC goes back to 2012, not merely as a professional acquaintance, but as a satisfied and long-standing customer. Over the years, I have seen their consistent efforts in building knowledge platforms and creating meaningful engagement within the profession. **The Control Room** is their most ambitious step yet, **a dedicated space for India's internal audit practitioners to think out loud, share what they have truly learned, and shape the profession together**. When Manesh Karani asked me to write its inaugural piece, I simply could not say no.

For me, Internal Auditing has been a fascinating journey of learning, unlearning, and understanding human behaviour in organisations. Having spent decades in audit leadership and now serving as Chair of Audit Committees on multiple Boards, my perspective has naturally evolved. Earlier, I viewed Internal Audit from an "inside-out" approach. Today I observe it increasingly from an "outside-in" perspective. This transition itself has been a profound learning.

a. The changing role of the Internal Auditor

Today's Internal Auditor cannot remain confined to Standards, checklists, and compliance frameworks alone. Those are essential foundations, but they are no longer sufficient. Domain knowledge is becoming as important as audit knowledge itself. Simultaneously, expectations in Information Technology, data analytics, cyber risks, and Artificial Intelligence are rising exponentially. Internal Auditors who fail to understand AI may soon find themselves auditing systems they do not fully comprehend.

b. From Three Lines to Free Lines

Another important evolution relates to the traditional Three Lines of Defence, which over time became the Three Lines Model. I believe it is time to go further. Today's Internal Auditors must start embracing what I call the "Free Lines" approach.

What do I mean by that? **Internal Auditors must free themselves from rigid functional silos and narrow thinking. They must think like business leaders first, controls specialists second, and trusted governance partners always.** Unless an auditor understands business realities, commercial pressures, growth aspirations, and competitive dynamics, **audit observations may remain technically correct but strategically irrelevant.**

"Think like business leaders first, controls specialists second, and trusted governance partners always."

c. Engagement, communication & the glass ceiling

Equally important is the Internal Auditor's ability to build meaningful engagement with the Audit Committee and the Board. Good audit reports are not enough. Communication, clarity, business relevance, and maturity of judgement matter enormously. **Unfortunately, many talented Internal Auditors hit a glass ceiling early in their careers. Under the label of "independence," roles become functionally isolated, and the profession fails to receive the organisational importance it deserves.**

Therefore, every smart Internal Auditor must consciously build broader managerial capabilities. **Internal Auditors should not hesitate to move into business, operations, risk management, strategy, or leadership roles whenever opportunities emerge.** Such cross-functional exposure enriches both the individual and the profession.

The era of remaining low-profile, overly suspicious, and mechanically fault-finding is behind us. The future belongs to Internal Auditors who are balanced, technology-savvy, commercially aware, ethically grounded, and capable of influencing organisational direction positively.

d. A word to the next generation

The challenges before the profession are significant, but so are the opportunities. To the younger generation entering this exciting profession, I extend my very best wishes. **For those willing to continuously learn, adapt, evolve, and contribute meaningfully, Internal Auditing can offer an extraordinarily fulfilling and impactful innings.**

I look forward to the conversations this column will spark. The Control Room is built for exactly this, practitioners speaking honestly to practitioners, and I am proud to open that conversation.

"In today's world, the real illiterate is not the person who cannot read or write, but the one who fails to optimise and ride on Information and Technology with the steering wheel of Artificial Intelligence."

www.lasergrc.com

The Control Room is a global internal audit community, built for the future of the profession by Laser GRC. To contribute to a future edition, write to thecontrolroom@lasergrc.com

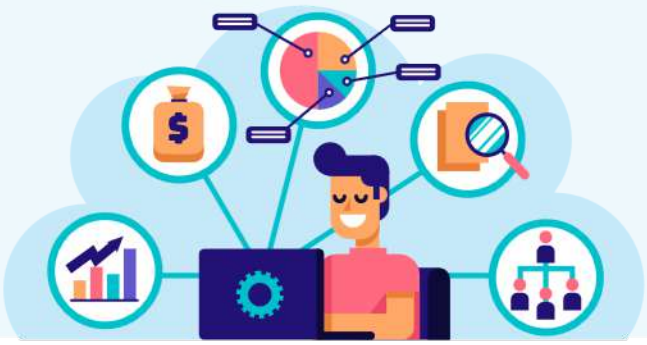
Jeevan Velayudhan
Co-Founder & Director.
MMM Info Solutions Pvt. Ltd

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

LEADER IN SPOTLIGHT

INTERNAL AUDIT AWARENESS MONTH

Leaders Spotlight: Series 01

INTERNAL AUDIT:

MORE THAN JUST NUMBERS.

Featured Leader:

ASHISH JAIN

CAIO, Nayara Energy

EXPERIENCE

2+ decades in Assurance, Risk Consulting, Controllership, Compliance & Ethics, Forensics, Governance & Strategy

LEADERSHIP ROLES

Former Shell Group leader; served on IAC – WIRC of IAIC & Board of Governors –IIA Mumbai Chapter

LEADERSHIP SPOTLIGHT SERIES

ASHISH JAIN

WHY I CHOSE IA?

- What started as a temporary 2-month assignment turned into a journey of continuous learning, exposure, and impact.
- From day one, Internal Audit gave me opportunities to understand businesses deeply, solve challenges, and add real value to organizations.
- In IA, there is never a dull day — and that's what makes this journey so rewarding.

A MYTH I BROKE?

"That Internal Auditors don't understand business dynamics."

- I believe effective Internal Audit is not just about identifying gaps — it's about truly understanding the business, its operations, and the environment it works in.
- The stronger the business insight, the greater the value an auditor can bring.
- Understanding the business is not optional for an auditor — it's essential for impact.

SKILL THAT MATTERS *most?*

While Internal Audit requires many competencies, two skills stand above the rest for me — strong stakeholder management and analytical thinking.

- **Strong Stakeholder Management**
  The ability to build trust, communicate effectively, and collaborate across functions to drive results.
- **Analytical Thinking**
  The ability to analyze deeply, connect dots, and turn data into meaningful insights.

MY DAILY SUPERPOWER?

Agility, resilience, and objectivity.

- **AGILITY**
  The ability to adapt quickly, embrace change, and navigate evolving business landscapes.
- **RESILIENCE**
  The strength to stay focused, bounce back from setbacks, and keep moving forward.
- **OBJECTIVITY**
  The commitment to remain unbiased, evidence-based, and driven by facts and integrity.

MY MESSAGE TO YOUNG AUDITORS

- If you can turn your achievements into passion, your career journey will become both rewarding and fulfilling.
- Stay curious, keep learning, and never stop growing.
- Never underestimate the impact you can create through Internal Audit.

INTERNAL AUDIT AWARENESS MONTH

Leaders Spotlight: **Series 02**

LEADING BEYOND COMPLIANCE

Featured Leader:

AMIT SHARMA

Vice President
(Risk Management & Internal Audit)
Welspun Corporate Services Limited

EXPERIENCE

20+ years in the GRC journey.

LEADERSHIP ROLES

Global exposure.
Built Internal Audit functions from the ground up.

"Amit Sharma represents leadership that goes beyond compliance — driving governance, strengthening businesses, and creating lasting impact across organizations."

INTERNAL AUDIT AWARENESS MONTH

LEADERSHIP SPOTLIGHT SERIES

AMIT SHARMA

WHY I CHOSE IA?

I like helping people.
IA gives me a platform to help organizations and individuals improve **Corporate Governance** by:

- Enhancing Process Maturity
- Proactive Risk Management
- Implementing Efficient Internal Controls

"This gives me a lot of satisfaction personally."

A MYTH I BROKE?

Auditors can be trusted and collaborated by businesses to achieve growth.

- Builds Trust
- Stronger Collaboration
- Better Decisions & Risk Management
- Sustainable Business Growth

"When auditors and business teams work together, organizations grow stronger."

SKILL THAT MATTERS *most?*

Listening is the first step to true understanding.

As audit professionals, we need to hear people a lot. Unless we understand why someone is doing what they are doing, we can't justify our role.

- Hear beyond words
- Understand the real context
- Add value with insight
- Build trust and collaboration

MY DAILY SUPERPOWER?

I start my day with 2 things:

1. I listen to soft music for 10–15 minutes
It calms my mind, boosts focus, and sets a positive tone for the day.

2. I check my mood meter
It helps me reflect, realign, and respond better to myself and to others.

A calm mind. A clear check-in.
A powerful me.

"Small habits. Big impact. That's my daily superpower."

MY MESSAGE TO YOUNG AUDITORS

Focus on your Stakeholder Management and Communication Skills to achieve success.

- Why it matters
- Communicate with Clarity
- Collaborate Effectively
- Navigate Expectations
- Drive Better Outcomes

"Your ability to connect is your greatest professional asset."

INTERNAL AUDIT AWARENESS MONTH

Leaders Spotlight: Series 03

INSPIRING TRUST. DRIVING IMPACT.

Featured Leader:

POOJA BHUTRA

Director

Stewardship and Governance
Procter & Gamble

EXPERIENCE

15+ years of experience in Internal Audit, Governance, Risk Management, and Controls.

LEADERSHIP ROLES

Currently leading Stewardship and Governance at Procter & Gamble, Passionate about designing controls and helping build compliant business processes.

Proven track record of driving enterprise-wide initiatives that enhance governance, mitigate risk, and build sustainable value.,

LEADERSHIP SPOTLIGHT SERIES

POOJA BHUTRA

WHY I CHOSE IA?

- One of the biggest reasons I chose Internal Audit was the commercial understanding it offers.
- There's a unique satisfaction in understanding how a business actually works and then helping teams with practical and relevant solutions.
- Internal audit gives access to wide variety of functions, businesses so there is never a dull day. This leads to enormous opportunity to keep learning and growing in your careers

A MYTH I BROKE?

- One myth I've tried to break is that auditors are only there to find issues and escalate them to senior leadership.
- Early on, I learned that the role of an Internal Auditor goes beyond identifying problems — it's about helping businesses understand the impact of those issues and guiding them toward practical and viable solutions.
- In simple words, I've tried to break the myth that auditors are just "policing" functions.

SKILL THAT MATTERS *most?*

- **Analytics**
  Knowing how to slice and interpret data in a way that provides meaningful insights and helps connect the dots.

- **Influencing Stakeholders**
  Simply sharing a report is not enough. The real impact comes when stakeholders truly understand the issue and are willing to act on it.

MY DAILY SUPERPOWER?

I start my day with 2 things:

- I think my daily superpower is the ability to sense issues even through casual corridor conversations and then connect those observations with data.That combination has always given me an edge.
- Also, I strongly believe that subject matter expertise is a superpower. Knowing the right things at the right time is key in Internal Audit and governance in general.

MY MESSAGE TO YOUNG AUDITORS

- Always be authentic and never hesitate to ask questions while auditing.
- Internal Audit is one field that gives you the opportunity to learn almost every business process, and much of that learning comes directly from process owners themselves.
- Once you build that knowledge, there is no looking back.
- Stay curious, stay hungry to learn, and everything else will follow.

INTERNAL AUDIT AWARENESS MONTH

Leaders Spotlight: Series 04

EMPOWERING ASSURANCE. STRENGTHENING BUSINESS RESILIENCE.

Featured Leader:

HARDIK DESAI

Head – Internal Audit & JSOX
Yokohama Group
(ATC Tires India Pvt Ltd)

EXPERIENCE

15+ years of experience in Internal Audit, Risk Management, Internal Controls, and JSOX Compliance.

LEADERSHIP ROLES

Leading Internal Audit and JSOX initiatives at Yokohama Group (ATC Tires India Pvt Ltd). Expertise in strengthening governance frameworks, enhancing compliance culture, and improving operational efficiency.

Proven ability to identify process gaps, mitigate risks, and support strategic decision-making. Strong partner to leadership teams in driving accountability, transparency, and business resilience.

INTERNAL AUDIT AWARENESS MONTH

LEADERSHIP SPOTLIGHT SERIES

HARDIK DESAI

WHY I CHOSE IA?

It's more than a profession — it's where curiosity meets impact.

- Understanding how businesses work
- Improving processes & controls
- Managing risks effectively
- Learning something new every day
- Creating real business value

A MYTH I BROKE?

Many people think auditors are only here to find mistakes.
But I've always believed Internal Audit is here to protect, improve, and support.

- Building trust with teams
- Improving business processes
- Strengthening controls
- Supporting better decisions
- Creating long-term value

The biggest win for me?
When people walk out of an audit feeling more confident about their function — not afraid of it.

SKILL THAT MATTERS *most?*

People often say the most important audit skills are:

- Data Analytics
- Risk Assessment
- Technical Knowledge

They matter — but for me, the real skill is Listening.

- Listening to understand, not to judge
- Hearing what is said — and what isn't
- Building trust before asking questions
- Understanding people beyond the checklist

MY DAILY SUPERPOWER?

Staying calm when conversations get uncomfortable.

Audit discussions can be difficult. People can feel defensive when findings impact their area.
But over time, I've learned that how you deliver a finding matters just as much as the finding itself.

- Stay calm under pressure
- Keep conversations constructive
- Make people feel heard
- Focus on solutions, not blame
- Build trust through communication

MY MESSAGE TO YOUNG AUDITORS

Don't just try to sound like an auditor. Try to understand people.

- Technical skills can be learned
- Frameworks & standards will come with time
- But curiosity and communication make the real difference

The best auditors are the ones who:

- Ask thoughtful questions
- Stay curious
- Challenge comfortable answers
- Build genuine conversations
- Bring a point of view to the table

INTERNAL AUDIT AWARENESS MONTH

Leaders Spotlight: **Series 05**

INSIGHT TODAY. RESILIENCE TOMORROW.

Featured Leader:

LALU CHAUHAN

AVP – Internal Audit

Reliance Infrastructure Ltd.

EXPERIENCE

20+ years of experience in Internal Audit, Risk Management, Compliance, and Governance.

LEADERSHIP ROLES

Expertise in risk assessment, internal controls, fraud risk management, and process improvement. Skilled in SOX compliance, internal audit methodologies, and data-driven analytics.

Strong track record in stakeholder management, audit strategy, and assurance excellence. Committed to ethical practices, continuous learning, and creating a culture of accountability.

INTERNAL AUDIT AWARENESS MONTH

LEADERSHIP SPOTLIGHT SERIES

LALU CHAUHAN

WHY I CHOSE IA?

Internal Audit gives you a panoramic view of an entire organization.

- Understanding strategy & operations
- Learning how businesses truly function
- Solving problems across departments
- Interacting with people at every level
- Creating impact beyond numbers

One day you're speaking with the security guard at the gate, and the next day you're presenting insights to the MD or Board members.

A MYTH I BROKE?

The biggest myth?
That auditors are just "corporate policemen" who come to point fingers.

Modern Internal Audit is much more than that.

- Building trust with stakeholders
- Solving risks collaboratively
- Supporting better decisions
- Strengthening processes
- Becoming a trusted business partner

SKILL THAT MATTERS *most?*

For me, the most important skill in Internal Audit is:

- Active Listening
- Strong Business Acumen

Why it matters

- Understanding the "why" behind decisions
- Connecting risks with business goals
- Listening beyond surface-level answers
- Giving practical recommendations that actually work

MY DAILY SUPERPOWER?

An Open Mind • Curiosity • Empathy

One moment, you're understanding operations on a factory floor, and the next, you're discussing strategy in a boardroom.

- What keeps me effective
- Listening without bias
- Adapting quickly to changing situations
- Staying curious and continuously learning
- Understanding different perspectives with empathy

MY MESSAGE TO YOUNG AUDITORS

- Stay curious
- Look beyond the checklists
- Understand how the business truly works
- Keep learning every day
- Adapt to IT & AI-driven tools

Internal Audit is not just about finding mistakes. It's about helping organizations grow safely and sustainably.

INTERNAL AUDIT AWARENESS MONTH

Leaders Spotlight: Series 06

ASSURANCE TODAY. IMPACT TOMORROW. VALUE ALWAYS.

Featured Leader:

PRATIMA MALLICK

Asia Pacific Zone – Internal Audit
Elevator Company

EXPERIENCE

Over 16 years of experience in Internal Audit, Risk Management, and Assurance

LEADERSHIP ROLES

Leading audit strategies, risk assessments, and control evaluations across diverse functions

Proven track record in building high-performing teams and fostering a culture of accountability

Passionate about continuous improvement and delivering measurable impact

INTERNAL AUDIT AWARENESS MONTH

LEADERSHIP SPOTLIGHT SERIES

PRATIMA MALLICK

WHY I CHOSE IA?

I was introduced to Internal Audit during my articleship while working across taxation, statutory audits, secretarial work, and IA assignments.

What attracted me to Internal Audit?

- Exposure beyond numbers and compliance
- Understanding how businesses truly operate
- Learning across industries & geographies
- Gaining insights into real business challenges
- Contributing towards stronger processes and controls

A MYTH I BROKE?

Myth
At the beginning of my career, I believed auditors were meant to find mistakes and play the role of the "bad cop."

Truth
With experience, my perspective completely changed.

Internal Audit is:

- Not about criticizing people
- About partnering with the business
- Solving problems with transparency
- Protecting the organization from risks

SKILL THAT MATTERS *most?*

Learning how to collaborate with the business while staying ethical, objective, and true to my principles.

What helps me grow

- Building strong business relationships
- Maintaining independence and integrity
- Balancing collaboration with accountability
- Creating trust through transparency

MY DAILY SUPERPOWER?

Transparency and the courage to speak difficult truths.

What defines my strength

- Being honest even in uncomfortable situations
- Staying objective under pressure
- Communicating with clarity and integrity
- Focusing on what is right for the organisation

MY MESSAGE TO YOUNG AUDITORS

Never compromise your ethics for short-term comfort, pressure, or approval.

- Integrity builds lasting credibility
- Values matter more than temporary success
- Honest auditors earn long-term trust
- Always work in the best interest of the organisation

THE INSIGHT EXCHANGE AUTHOR'S CANVAS

gentic udit:

Transitioning from utomated Testing to utonomous I udit Workflows

In recent years, organizations have increasingly relied on automation to streamline software testing, compliance checks and internal audits. Automated testing frameworks have improved efficiency, reduced human error and enabled continuous monitoring of systems. However, automation still operates largely within predefined rules and scripts. As artificial intelligence (AI) continues to advance, a new paradigm is emerging – Agentic Audit, where autonomous AI agents actively plan, execute and refine audit workflows with minimal human intervention. This shift marks a transitions from static automation towards dynamic, intelligence auditing systems capable of adapting to complex environments.

From Automated Testing to Intelligent Oversight

Traditional automated testing focuses on executing prewritten scripts or rules to validate specific conditions. For e.g., automated compliance tests might verify whether financial transactions follow regulatory constraints or whether security policies are correctly implemented. While effectively, these systems depend heavily on predefined logic and require frequent updates as systems evolve.
Agentic audit systems go beyond this model. Instead of simply executing predetermined checks, AI agents can analyze system contexts, identify potential risk areas and design their own audit procedures. These agents combine machine learning, reasoning frameworks and orchestration capabilities to simulate the decision-making process typically performed by human auditors.

The result is a shift from rule-based verification to goal driven investigation. Rather than asking "Does this rule pass?", agentic agents ask "What areas of this system present the highest risk and how should they be examined?".

What Defines an Agentic Audit System?

Agentic auditing involves multiple AI agents collaborating to conduct comprehensive evaluations of systems, processes or datasets. These agents operate with specific capabilities such as planning, tool usage and learning from prior results.

A typical agentic audit workflow includes:

- **Objective Interpretation:** The AI agent interprets the audit objective, for e.g. verifying regulatory compliance, detecting anomalies in financial data, or evaluating cybersecurity

mit Sharma
Vice President & Head of udit
P C at EXL

posture.

- **Dynamic Audit Planning:** Instead of executing a fixed script, the agent generates an audit plan. It determines which datasets, logs or systems to analyze and prioritizes tasks based on risk indicators.

- **Autonomous Execution:** The system executes the audit by interacting with testing tools, querying databases, analyzing logs or running simulations.

- **Iterative Investigation:** If anomalies are detected, the AI expands the investigation automatically – collecting additional evidence, running deeper tests or cross-checking related systems.

- **Explaining Reporting:** Finally, the system generates structured reports explaining findings, risk levels and suggested remediation actions.

This approach enables continuous and adaptive auditing rather than periodic and static assessments.

Advantages of Agentic Audit workflows

The transition to agentic audit system offers several key advantages, such as:

- **Continuous & Proactive Auditing:** Traditional audits often occur periodically – quarterly, annually or during compliance reviews. Agentic systems can operate continuously, monitoring systems in real time and identifying potential issues before they escalate.

- **Improved Coverage and Depth:** Human auditors and static automation cannot examine every possible scenario in complex systems. AI agents can dynamically explore new patterns, simulate potential failures and test edge cases that were not previously defined.

- **Reduced Manual Overhead:** Audit teams often spend significant time gathering evidence, running checks and preparing documentation. Autonomous agents can automate much of this operational work, allowing human auditors to focus on interpretation, governance and strategic risk assessment.

- **Adaptive Learning:** Agentic systems can learn from past audits. When a new vulnerability or compliance issue is discovered, the systems incorporates this knowledge into future investigations, improving detection over time.

- **Faster Incident Detection:** Because these systems continuously analyze operational data, they can identify anomalies, such as unusual financial patterns, security breaches or significant process deviations, much earlier than periodic audits would have.

Key Technologies Enabling Agentic Audits

Several technological advancements are enabling the emergence of agentic audit workflows, such as:

- Large Language Models (LLMs) provide reasoning and interpretation capabilities that allow agents to understand policies, regulations and audit objectives written in natural language.
- Tool-Orchestrating AI agents enable systems to interact with databases, testing frameworks, monitoring tools and analytics platforms.
- Knowledge Graphs and Data Lineage Systems help agents trace how data flows across systems, which is essential for financial, operational and regulatory audits.
- Anomaly Detection Models identify unusual patterns in large datasets, flagging areas that require deeper investigation.
- Combined, these technologies create AI systems capable of conducting complex, multi-step audit processes with minimal manual direction.

Governance and Trust Considerations

Despite its advantages, the adoption of agentic auditing raises important governance questions. Autonomous systems must be transparent, explainable and accountable. Organizations must ensure that AI driven audit findings can be validated and traced.

Human oversight remains essential. Instead of replacing auditors, agentic systems function as intelligent collaborators that augment human expertise. Auditors still define objectives, review findings and ensure ethical and regulatory compliance.

Another critical challenge is model bias and reliability. If the underlying AI models are poorly trained or misaligned with regulatory frameworks, they could overlook risks or generate misleading conclusions. Therefore, organizations must establish validation frameworks and monitoring mechanisms for the AI agents themselves.

Implementation Challenges and potential solutions

Transitioning to agentic audit workflows is not trivial. Organizations often face several challenges, such as:

- **Data fragmentation:** Audit data is often dispersed across multiple enterprise systems, limiting the ability of AI agents to access and analyze information consistently.
- **Legacy infrastructure:** Many organizations still rely on legacy systems that lack APIs or integration capabilities required for AI-enabled workflows.

- **Regulatory acceptance:** Regulators may require transparency, explainability, and robust assurance mechanisms before relying on AI-driven audit processes.
- **Cultural resistance:** Audit professionals may initially hesitate to trust autonomous or semi-autonomous systems for critical oversight functions.
- **Risk of Over-automation:** Excessive reliance on AI without adequate oversight may weaken professional judgment and accountability.

Overcoming these challenges requires thoughtful strategy and effective execution. Organizations can consider the following measures to mitigate some of the challenges outlined above:

- **Strengthen System Observability:** Ensure systems generate detailed logs, metadata, and audit trails to enable transparent analysis by AI agents.
- **Phased Implementation Approach:** Begin with low-risk, repetitive tasks such as data aggregation, control testing, or anomaly detection before expanding to more complex audit activities.
- **Human-in-the-Loop (HITL) Controls:** Allow AI agents to perform data gathering and preliminary analysis while human auditors review critical findings and exercise professional judgment.
- **Modernize Integration Capabilities:** Use APIs, middleware, or data integration layers to connect legacy systems with AI-enabled audit tools.
- **Establish Robust Governance Frameworks:** Implement strong data security, privacy protections, model validation processes, and ethical guardrails to ensure responsible and compliant AI adoption.

The Future of Autonomous Auditing

As AI technologies mature, agentic auditing will likely become a core component of enterprise governance, instead of periodic manual audits supplemented by simple automation, organizations will deploy networks of intelligent agents that continuously monitor operational, financial and technical systems.

Future agentic systems may even coordinate across departments, combining financial, cybersecurity, operational and compliance auditing into a unified intelligence layer. Such, systems could identify systemic risks that traditional audits might miss.

Additionally, advancements in explainable AI will improve trust and transparency, allowing regulators and stakeholders to understand how audit conclusions were reached.

Conclusion

Agentic audit represents a significant evolution in how organizations approach verification, compliance and risk management. Moving beyond traditional automated testing, autonomous AI agents can dynamically plan, execute and refine audit processes. While, challenges related to governance, integration and trust remain, the potential benefits including continuous monitoring, deeper insights and reduced manual efforts are substantial.

Rather than replacing human auditors, agentic systems will redefine their role. Auditors will increasingly acts as supervisors of intelligent systems, focusing on interpretation, strategy and ethical oversight. As organizations navigate increasingly complex digital environments, agentic audit workflows may become the foundation of next generation assurance and accountability systems.

The Ethical uditor in the ge of rtificial Intelligence

Reframing assurance, accountability, and judgement in an algorithmic economy

When speed outpaces judgement

Artificial Intelligence is no longer confined to innovation pilots or experimental use cases. Across organisations—particularly startups, unicorns, and high-growth enterprises—AI now operates at the centre of decision-making. Credit approvals, fraud detection, hiring shortlists, pricing engines, customer targeting, and risk scoring are increasingly shaped by algorithms rather than individuals.

This acceleration reflects a broader shift in the new economy. Business models privilege speed, scalability, and automation. Decision cycles are compressed, experimentation is continuous, and technology stacks are cloud-native, data-intensive, and increasingly opaque to non-specialists. Governance frameworks, however, rarely evolve at the same pace.

As highlighted throughout the IA Today – April 2026 edition, this imbalance creates a critical tension. Organisations derive efficiency and insight from intelligent systems, but they simultaneously increase exposure to ethical, reputational, and regulatory risk. Stakeholders are no longer asking only whether systems function as designed—they are asking whether outcomes are fair, explainable, consistent with values, and defensible under scrutiny.

In this environment, internal audit faces a defining inflection point. Traditional assurance models—focused on compliance, control design, and operating effectiveness—remain necessary. But they are no longer sufficient. Artificial intelligence introduces risks that sit beyond policies, process maps, and control matrices. Addressing these risks requires professional judgement, contextual understanding, and a renewed emphasis on ethical stewardship.

This is where the concept of the Ethical Auditor becomes central—not as a new designation, but as the natural evolution of the profession's enduring purpose.

Ethics as an extension of enterprise risk

AI ethics should not be viewed as a philosophical overlay or a well-intentioned add-on to compliance programs. In practice, ethical failures surface as very real business risks—triggering regulatory scrutiny, eroding customer trust, weakening governance, and undermining long-term strategy.

From an internal audit perspective, ethical risk in

Rahul Mishra
Senior Manager
I F , Protiviti India

AI-enabled environments typically concentrates in three interconnected areas.

1. Bias embedded at scale

AI systems learn from historical data. Where legacy processes, social structures, or past decision-making have embedded bias, algorithms may replicate—or inadvertently amplify—those distortions. The danger is not isolated error; it is systemic unfairness executed consistently and at scale, often under the guise of objectivity.

Without explicit governance, challenge mechanisms, and ongoing testing, organisations risk institutionalising biased outcomes while assuming that automation has removed subjectivity.

2. Opacity and explainability gaps

Many AI models function as "black boxes." While inputs and outputs are visible, the internal logic driving decisions may be difficult to articulate. This creates acute challenges when organisations must explain outcomes to customers, regulators, audit committees, or courts.

In an era of heightened accountability, accuracy alone is no longer enough. Decisions must be explainable, reviewable, and capable of standing up to challenge.

3. Automation without accountability

In the pursuit of efficiency, human judgement is sometimes removed without redefining ownership. When automated decisions lack clear accountability frameworks, ethical risk escalates sharply. Errors become harder to challenge, responsibility becomes diffuse, and governance weakens precisely where decisions carry the greatest impact.

The ethical auditor's role is to surface these risks early—before they crystallise into regulatory findings or public controversy.

Reframing audit questions for intelligent systems

Historically, auditors have assessed whether rules were designed appropriately and applied consistently. AI-driven systems demand a broader and more nuanced line of enquiry—one that focuses as much on outcomes as on controls.

Key questions increasingly include:

- Who is accountable for algorithm-driven decisions?
- How are fairness, proportionality, and bias assessed and monitored?
- What ethical principles guide the choice to automate decisions?
- Can outcomes be clearly explained and defended to stakeholders?

This represents a shift from auditing transactions to auditing decisions. It does not replace traditional control testing, but it extends assurance into areas where governance, ethics, and organisational values intersect.

Privacy and the ethics of intelligent data use

Data protection regimes have matured across jurisdictions, yet AI introduces privacy dynamics that extend well beyond traditional compliance frameworks.

Key ethical considerations include:

- **Purpose drift:** data reused beyond its original or disclosed intent
- **Inference risk:** sensitive insights derived from seemingly non-sensitive data
- **Aggregation effects:** ethical implications arising when datasets are combined across domains

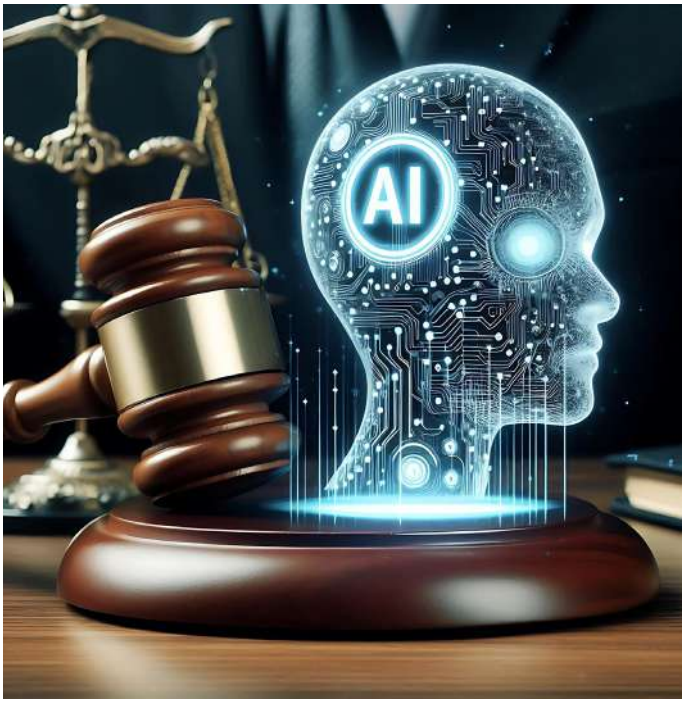
Auditors must therefore evaluate not only how data is collected and stored, but how its meaning, power, and impact evolve when advanced analytics are applied. Legal compliance may exist, yet ethical defensibility may not.

Practical insight: ethics beyond technical compliance

Consider a fast-growing digital lending platform that implemented AI-based credit scoring to accelerate approvals and reduce manual underwriting effort. The business objective was clear: improve customer experience, reduce turnaround times, and scale credit decisions without proportionately increasing underwriting teams.

From a conventional audit standpoint, the environment appeared well controlled. Data usage approvals were formally documented, models had undergone technical validation by data science teams, and access, change, and deployment controls operated effectively. On paper, the system met policy, compliance, and technology risk requirements.

However, when internal audit examined decision outcomes rather than model design, a different picture began to emerge. Portfolio-level analysis showed that certain customer segments experienced significantly higher rejection rates than others, even when traditional credit indicators were comparable. These patterns were not immediately visible in sample-based testing and only became apparent when outcomes were analysed across large datasets. Further, when customer grievances were reviewed, business teams struggled to explain individual credit decisions in a way that was understandable, consistent, and defensible. Explanations relied



heavily on technical language ("the model score was below threshold") rather than on customer-relevant reasoning. Compounding this issue, there was no defined escalation process to challenge outcomes that were technically correct but potentially unfair when viewed in aggregate.

Internal audit deliberately reframed the engagement—moving from a model assurance lens to a decision-governance lens. The discussion with management shifted from whether the model worked as designed to whether its outcomes aligned with the organisation's stated values, customer commitments, and risk appetite.

Practical recommendations focused on three governance enablers rather than technical re-engineering. First, the introduction of minimum explainability standards for customer-facing decisions, ensuring that rejection reasons could be clearly articulated and reviewed. Second, the establishment of human-in-the-loop escalation for edge cases and adverse outcome patterns, restoring accountable judgement where automation reached its limits.

Third, explicit executive ownership of algorithmic risk, with regular reporting to senior management and the board on decision fairness trends.

Importantly, nothing in the original design was non-compliant. Yet without these governance mechanisms, the organisation carried elevated reputational, regulatory, and trust risk. This illustrates where ethical assurance creates tangible value—by identifying risks that sit beyond compliance, but squarely within enterprise accountability.

Experience, judgement, and the human role in AI assurance

Debates around AI assurance often emphasise technical capability—model validation, analytics, and tooling. These are essential, but insufficient in isolation.

Ethical assurance relies even more heavily on attributes that have always defined effective auditors: professional scepticism, contextual understanding of the business, anticipation of unintended consequences, and credibility with boards and regulators.

Technology can enhance assurance. Judgement anchors it. As automation expands, the auditor's role shifts from gathering evidence to interpreting outcomes, challenging narratives, and ensuring that intelligent systems remain aligned with organisational intent.

Closing remarks: ethics as the next evolution of assurance

Artificial Intelligence does not diminish the relevance of internal audit—it heightens it.

As organisations delegate greater authority to machines, assurance functions must ensure that responsibility remains clearly assigned, decisions remain fair and explainable, and automation aligns with organisational values and societal expectations. In this environment, the internal auditor evolves from control reviewer to guardian of responsible decision-making.

The Ethical Auditor is not a new profession. It is the profession responding—once again—to where risk truly resides.

II India Delhi Branch

Celebrating a quarter of growth, innovation and impactful initiatives!
From engaging learning sessions, insightful publications to exciting upcoming events, the quarter highlights the continued efforts of IIA India - Delhi Branch towards advancing the Internal Audit profession.

Activity Highlights

Training Committee

The Committee successfully organized a webinar on "Labour Laws Unlocked: A Strategic Lens for Internal Auditors" with 110+ participants. CA Ruchi Gupta delivered an engaging session with practical insights and interactive discussions.

The Jaipur Audit Club of IIA India - Delhi Branch also hosted a webinar on: "Internal Audit Reimagined: Driving Excellence with Six Sigma & Analytics". The session focused on analytics-driven auditing and process excellence, attracting 105+ participants.

Upcoming in June 2026:
Webinar on "Practical Use of AI Tools in Internal Audit"

Conference & Events Committee

The committee is all set to organize the Annual Conference 2026 on 19th–20th June 2026 with the theme: "Audit Reimagined: Intelligence, Integrity & Impact"

The conference will feature visionary speakers, insightful sessions and networking opportunities for audit, risk and governance professionals.

Publication & Research Committee

The committee contributed insightful blogs on emerging audit themes:

1. The Expanding Role of Internal Audit in UAE" — Mr. Rajat Mohan
2. The New Cybersecurity Frontier: Internal Audit's Role in Assessing AI-Driven Threats and Quantum Computing Vulnerabilities" — Mr. Amit Sharma

Women's Forum

The forum contributed the blog:

1. "India's Invisible Economic Engine: Why Boards and Auditors Must Account for Unpaid Care Work" — Ms. Priya Gupta

IIA India - Delhi Branch continues to drive learning, innovation and thought leadership within the Internal Audit profession.

uditing I lgorithms:

Governance, Bias, and ccountability in I Models

Artificial Intelligence (AI) has rapidly transitioned from an experimental technology to a core decision-making engine across industries. From credit scoring and fraud detection to audit analytics and controls testing, AI models are increasingly shaping outcomes with real-world consequences. This shift demands a parallel evolution in assurance: auditing AI algorithms is no longer optional, it is foundational to governance, trust, and risk management.

The Institute of Internal Auditors highlights that internal auditors must play a dual role as advisors and assurance providers in helping organizations manage AI risks, design controls, and ensure alignment with strategic objectives.

AI Governance: From Principles to Enforceable Controls

Modern AI governance frameworks are no longer abstract ethical guidelines; they are multi-layered control systems integrating legal, technical, and organizational mechanisms.

At their core, governance frameworks are anchored in five principles:

- **Fairness** – preventing discriminatory outcomes
- **Transparency & Explainability** – enabling understanding of decisions
- **Accountability** – ensuring organizations, not algorithms, are responsible
- **Privacy & Data Protection** – aligned with laws such as the Digital Personal Data Protection Act, 2023
- **Safety & Robustness** – resilience against failures and adversarial risks

The IIA framework emphasizes governance through the Three Lines Model, where:

- Management owns AI risks (First Line)
- Risk & compliance monitor (Second Line)
- Internal audit provides independent assurance (Third Line)

Lifecycle-Based Governance

Effective governance spans the entire AI lifecycle:

- **Data Stage** – Ensuring data quality, representativeness, and absence of systemic bias
- **Model Development** – Controlled feature engineering and documentation (model cards, datasets)
- **Validation & Testing** – Fairness testing across demographic groups
- **Deployment** – Risk-based classification (e.g., high-risk models in banking)

Swapnil N. Mithapelli
Senior Manager
Protiviti India Member Private Ltd.

- **Monitoring** – Detecting model drift, bias drift, and performance degradation
- **Decommissioning** – Responsible retirement and data archiving

This lifecycle approach shifts AI governance from a one-time review to a continuous control environment.

India's Governance Initiatives

India is actively shaping responsible AI through:

- **Digital Personal Data Protection Act, 2023** – Focus on consent, data minimization, and accountability
- Guidelines and oversight from the **Reserve Bank of India** for AI use in financial systems
- Policy frameworks by **NITI Aayog** promoting ethical, inclusive, and responsible AI

Bias in AI

Bias in AI is not an isolated issue it is a systemic risk emerging from data, algorithms, and human decisions.

Key Types of AI related Bias

- **Data Bias:** Unrepresentative datasets lead to skewed outcomes. Example: Credit models trained on urban data disadvantaging rural applicants.
- **Historical Bias:** AI replicates past inequalities embedded in data.
- **Algorithmic Bias:** Optimization for accuracy or profit may unintentionally disadvantage minority groups.
- **Proxy Bias:** Indirect discrimination via variables like location or education acting as substitutes for sensitive attributes.
- **Measurement Bias:** Poor proxies (e.g., income as sole indicator of creditworthiness).
- **Feedback Loop Bias:** Self-reinforcing cycles from model outputs influencing future inputs.
- **Evaluation Bias:** Over-reliance on aggregate metrics masking subgroup disparities.

The IIA framework explicitly identifies biased or discriminatory outcomes as a key AI risk that must be addressed through governance and controls.

The Fairness Trade-off

A critical challenge: It is mathematically impossible to satisfy all fairness definitions simultaneously. This makes bias mitigation not just technical but strategic and ethical, requiring alignment with regulatory expectations and societal values.

Types of AI Models: Audit Relevance

Understanding AI model types is essential because audit approach varies with model complexity and risk:

- **Rule-Based Systems (Deterministic AI)** – Operates on predefined rules and logic, highly transparent and interpretable

Audit focus: Rule validation and completeness

- **Machine Learning Models** – This model learns patterns from historical data and includes supervised, unsupervised, and reinforcement learning (e.g., credit scoring, predictive analysis)

Audit focus: Data quality, bias, and feature selection

- **Deep Learning Models – (Neural Networks):** This is a multi-layered architecture capturing complex relationships and often considered "black box" systems (e.g. Image recognition, Speech processing and Advanced predictive modelling)

Audit focus: Explainability, robustness testing under various scenarios, and bias detection in output testing

- **Generative AI Models** – Create content rather than predict outcomes and includes large language models (LLMs), image, and code generators (e.g., Contract analysis, Code generation for analytics)

Audit focus: Hallucination and misinformation risk, output bias, and alignment with intended use

Accountability: From Explainability to Contestability

AI accountability extends beyond system design, it encompasses legal, ethical, and societal responsibility. Four Pillars of AI Accountability

- **Auditability** – Complete logging of decisions and processes
- **Traceability** – End-to-end visibility from data input to output
- **Explainability** – Interpretable reasoning behind decisions
- **Contestability** – Ability for users to challenge outcomes

This is especially critical in high-impact sectors like banking, where regulators such as the Reserve Bank of India require explainable and fair AI decisions.

Auditing AI Algorithms: A Structured Approach

Auditing AI is fundamentally different from traditional IT audits. It requires a multi-layered, lifecycle-based audit methodology.

- **Data Audit -** Assess data quality, completeness, and representativeness, Review data lineage and sourcing and identify underrepresented or excluded populations

- **Model Audit:** Evaluate algorithm design and feature selection, detect proxy variables and hidden bias and assess robustness and sensitivity to input variations

- **Output Audit:** Test outcomes across demographic segments, apply fairness metrics (e.g., statistical parity, equal opportunity) and validate accuracy vs fairness trade-offs

- **Governance & Compliance Audit:** Verify adherence to laws and regulatory frameworks, review policies, documentation, and approval processes and assess alignment with organizational risk appetite

- **Continuous Monitoring:** AI models evolve, so must audits. Continuous auditing includes, Real-time dashboards, Drift detection systems and Incident reporting mechanisms

The IIA emphasizes that AI assurance provides "reasonable assurance," not absolute certainty, given the complexity and evolving nature of algorithms.

The "Black Box" Challenge

One of the most critical risks in AI auditing is the black box problem, where decision logic is not fully interpretable.

The IIA recommends addressing this through:

- Explicit documentation of unknowns
- Disclosure of limitations to stakeholders
- Use of alternative models or explainability tools
- Escalation of risks to governance bodies

In practice, this means auditors must often audit around the model, focusing on inputs, outputs, and controls rather than internal logic alone.

AI in Auditing: A Double-Edged Transformation

AI is not only being audited it is also transforming the audit function itself.

AI Use Cases in Audit

- Rule-based AI / RPA – Data collection and process automation
- Machine Learning – Anomaly detection and predictive analytics
- Natural Language Processing (NLP) tools – Contract analysis and control reviews
- Deep Learning – Image-based inventory verification
- Generative AI – Audit documentation and code generation

AI systems are not just technological tools they are decision-making agents embedded in socio-economic systems.

The Road Ahead: Bridging Principles and Infrastructure

AI governance is evolving toward:

- Standardized audit frameworks and certifications
- Regulatory enforcement across jurisdictions
- Governance-as-code embedded in systems

Independent AI audit ecosystems

However, challenges remain:

- Limited transparency in third-party models
- Trade-offs between privacy and fairness
- Global data imbalance affecting model performance

To conclude auditing AI algorithms therefore requires a shift:

- From static audits → continuous assurance
- From compliance → ethical accountability
- From system focus → human impact focus

Internal auditors, guided by frameworks like those from the Institute of Internal Auditors, are uniquely positioned to bridge this gap ensuring that AI innovation is balanced with governance, fairness, and trust. In the end, the objective is not to eliminate all AI risk that is unrealistic. The goal is to make AI risks visible, measurable, and manageable in alignment with organizational and societal values.

II India Hyderabad Chapter

The Annual Conference 2026 hosted by IIA India Hyderabad Chapter & Vizag Audit Club was a remarkable coming together of minds, ideas, and purpose celebrating the true essence of Internal Audit: efficiency, quality, strength, and impact.

We kicked off the day on a high note with vibrant energy brought into the room by our host, Deepika Santdasani, who has a remarkable ability to keep the audience engaged and energized throughout.

The tone for the day was set brilliantly by Madhuri Krishnaswamy and Krishnan Venugopal, who articulated the journey and vision of IIA with clarity and passion.

We were truly inspired by Dr. Amar Patnaik, whose insightful address left a lasting impression on everyone present.

The conference featured an exceptional lineup of sessions and discussions:

- Internal Audit – Amplified by Rajeev K., highlighting how audit functions can evolve to deliver greater strategic value.
- An engaging panel on "Bridging Expectations: Internal Auditors and the Board" with Arpit Garg, Saket Kumar Agarwal, Debasis Patri, Amit Jain, and Lalitha Satheesh sharing perspectives on aligning audit insights with boardroom priorities.
- Next Gen IA: From Possibility to Reality by Rahuul Rekhi, exploring the future-forward transformation of internal audit.

- A thought-provoking panel on "Internal Audit in the Age of Impact: From Scorekeeper to Game Changer" featuring Venkata Chaitanya, FCA, CISA, CFE, PGDCLCF, Sivaram Subramoniam, Gaurav Bhatia, and AMAN GUPTA emphasizing the shift towards value creation and strategic influence.
- Impact Through Adaptability: Evolving how you work by @Deepa Rao, inspiring professionals to evolve their thought process
- Risk Outlook - a compass to India's landscape by Srikanth Potturi, offering insights into navigating an ever-changing risk environment.
- A proud moment recognizing our newly certified CIAs, celebrating excellence and commitment to the profession.

The event concluded with a heartfelt vote of thanks by George Kalliath.
Heartfelt Thank You:

- To the entire BOG for their untiring efforts and unwavering commitment in making this event truly exceptional - Madhuri Krishnaswamy George Kalliath Bikram Jena Sunil Rao Deepika Santdasani Tinku Padia Amit Jain Venkata Chaitanya, FCA, CISA, CFE, PGDCLCF Rajeev K. Rana Bhaumik CA Dayaniwas Sharma (Daya) Arjun Golar and Ravi Namagri
- To our sponsors #SBI #EY #PwC #Protiviti #KPMG #Bakertilly #RiskMan #Global Professional Certifications
- To our esteemed speakers for sharing such powerful and thought-provoking insights.

To the entire Internal Audit fraternity for your overwhelming presence and support. With 260 registrations, an impressive 30% increase over last year - you truly made this event a grand success.

An outstanding show, an engaged audience, and a thoughtfully curated agenda made this conference truly memorable!

Board Expectations Reset

How udit Committees View I-Enabled ssurance Functions

Artificial intelligence (AI) is reshaping the way internal audits and the risk assurance functions operate. AI is increasingly providing continuous, data-driven, automated assurance. However, boards remain cautious. The real question is no longer whether AI can improve assurance but whether boards are ready to rely on it.

Trust Vs. Cost

The argument in favor of AI in assurance is straightforward. Conventional audit approaches rely on testing of limited samples of transactions and periodic analysis of information. AI, by contrast, can evaluate datasets in real time, identify anomalies, and flag risks. The efficiency gains are evident.

However, efficiency comes at a cost—and not just a monetary one. Beyond the technology and training investments, AI requires trust capital. The pressing question from boards is no longer "Can we afford this?" but "Can we rely on it?"

Whether AI works is not the primary concern. Whether the organization fully understands how it operates in practice is. How confident can a board be when an AI tool flags a vendor as high-risk or classifies a financial control as effective? And if such an output later proves inaccurate, who is accountable - the technology, or those who relied on it?

Audit Committees View

At the apex of governance sit audit committees. They are responsible for overseeing financial reporting, internal controls and risk management. They are experienced and seasoned, often with deep expertise in finance, law and business strategy, but not necessarily in data science or algorithm design.

This creates a real tension.

On the one hand, many committees recognize AI's potential. They increasingly question why assurance functions still rely on sampling when technology can test entire populations. They expect faster insights and earlier detention of risk.

They cannot directly question an algorithm to explain its reasoning. They cannot easily assess whether a model has been trained on appropriate data, or whether it can identify a new forms of risk that it has not previously encountered.

As a result, audit committees now expect AI-enabled assurance teams to deliver three things:

Rajat Mohan

Chartered ccountant and an alumnus of IIM hmedabad, and a Partner at MRG Global.

- **Transparency :** Clear, non-technical explanations of how conclusions are reached.
- **Responsibility:** Defined ownership for AI-driven decisions and errors.
- **Relevance:** D emonstrable improvement in assurance outcomes.

The Moment of Human Intervention Still Matters

Professional judgement remains one of the most critical elements that AI cannot replicate. AI can recognize patterns, but not always understand their context. It can raise alerts, but it cannot determine whether an anomaly represents a genuine risk or a legitimate exception. This is where human expertise is not merely helpful, but is essential.

Seasoned auditors and risk professionals possess something AI lacks - the ability to ask the right follow-up questions. An AI system may generate a finding, but interpreting that finding requires skilled human judgement by someone who can challenge it and decide whether it is justified.

Eliminating this layer of human oversight in pursuit of speed a cost efficiency would be a mistake.

Audit committees understand this. They do not want AI to replace professional judgment; they want it to augment it. Organizations that earn the greatest trust from their boards are those that clearly define where AI is applied, where human validation is required, and why those boundaries exist.

An Opportunity Rather than a Threat

It is not. Audit committees are not opposed to AI; they are opposed to being asked to trust something they not fully understand. That is a reasonable position, and assurance leaders should treat it as such.

AI has, in fact, reset expectations. But this reset presents an opportunity. Assurance functions are receiving more board attention than ever before. Committees are asking deeper questions, engaging more actively, and demanding higher standards of insight. For chief audit executives and risk leaders, this represents a chance to elevate their role—moving from a compliance-focused function to a true governance partner.

Assurance leaders must explain AI in terms boards understand—not technical depth, but through governance impact. Clarity builds confidence far more effectively than technical sophistication.

Conclusion

AI is not going away, and nor should it. Its ability to process vast volumes of data, detect risk in real time, and support faster, better-informed decisions is genuinely valuable. It may also operate at a lower marginal cost than human resources; with no absenteeism or variability in output. However, in governance and assurance, value is realized only when it is TRUSTED.

Audit committees globally are midway through the journey toward AI-enabled assurance. They are not asking organizations to slow adoption. They are asking to be brought along on the journey. Organizations that invest as much in explaining their AI systems as they do in deploying them will find that this expectation reset is not a burden to manage, but a platform to build upon.

The Institute of Internal Auditors
Madras Chapter

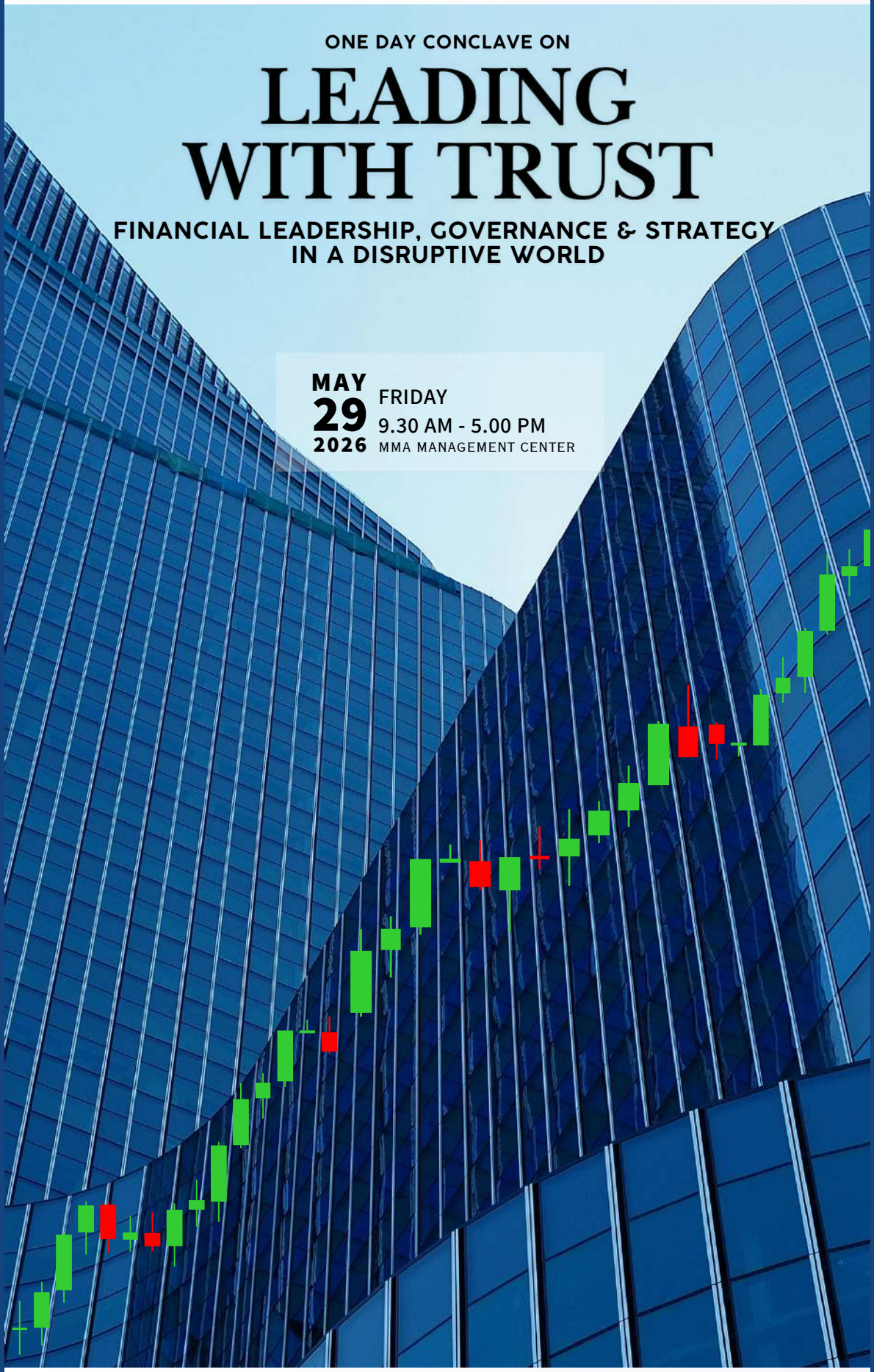
MADRAS MMA MANAGEMENT ASSOCIATION
ESTD 1956

ONE DAY CONCLAVE ON

LEADING WITH TRUST

FINANCIAL LEADERSHIP, GOVERNANCE & STRATEGY IN A DISRUPTIVE WORLD

MAY 29 2026 FRIDAY
9.30 AM - 5.00 PM
MMA MANAGEMENT CENTER



ROUTE MAP TO MMA - CLICK TO VIEW

udit of I vs. I in udit

Drawing the Line Between ssurance and Enablement

Background: Internal audit has always evolved in step with the organisation it serves. Its methodology has evolved: from working papers to data analytics, from financial control to governance, risk, and culture. Each shift required the profession to revisit its foundational assumptions while holding firm to its core purpose: to provide independent, objective assurance and advisory services that add value and improve an organisation's operations.

Artificial Intelligence and Internal Audit: Across the corporate landscape and globally, AI is reshaping how organisations take decisions, manage risk, interact with customers, report financial results, and comply with regulation. The internal audit function sits at the intersection of all these developments. It is asked simultaneously to provide assurance over the AI systems the organisation has deployed, and to deploy AI systems of its own to conduct that work and its other audit activities more effectively. These are two distinct responsibilities, and the internal auditor who conflates them or who addresses one while ignoring the other will fall short of the standard the profession and its stakeholders rightly expect.

The Distinction: Audit of AI versus AI in Audit: The starting point for clear thinking about AI in the context of internal audit is a precise articulation of the two phenomena at issue.

Aspect	Audit of AI	AI in Audit
Definition	The responsibility of internal audit to examine, evaluate and report on the AI systems deployed by the organisation as part of its processes, controls, and governance.	The internal audit function's own use of AI-powered tools within its audit practice.

ditya Kumar S.

Partner, R.G.N. Price & Co.,

Chartered ccountants

Aspect	Audit of AI	AI in Audit
Definition	The responsibility of internal audit to examine, evaluate and report on the AI systems deployed by the organisation as part of its processes, controls, and governance.	The internal audit function's own use of AI-powered tools within its audit practice.
Scope	Includes systems such as a bank's machine learning-based loan approval, AI-driven inventory management in manufacturing, or financial entities using large language models for regulatory disclosures	Encompasses platforms for data analytics, machine learning models for risk assessment and control testing, robotic process automation for data handling, natural language processing for document review, and continuous monitoring for real-time audit signals.
Mandate	Falls under the assurance mandate of internal audit.	Serves to enhance audit coverage, depth, and efficiency, but does not itself constitute assurance
Audit Objectives	Assess if systems are fit for purpose, governed properly, subject to adequate controls, producing reliable outputs, and operating within the risk appetite of the organisation.	Tools assist the auditor but do not replace the professional judgement required for forming the audit opinion.
Role	Provides assurance over organisational AI systems.	Enables and supports audit activities.

The differences between the two are not merely definitional. They carry distinct professional obligations, requiring distinct competencies, and produce distinct deliverables. The audit of AI produces assurance opinions and advisory findings directed at management and the Board on the organisation's AI governance. AI in audit produces improved audit procedures that ultimately support assurance opinions on the areas under review. Failing to distinguish between these may lead to insufficient auditing of the organisation's AI systems and an excessive dependence on the function's internal AI tools. In smaller organisations, where resources and expertise are shared, the temptation to conflate is greatest and the governance discipline required to resist it is correspondingly more important, not less.

The COSO Framework: Reading AI Through an Established Lens: The COSO Internal Control Integrated Framework (2013) and the COSO Enterprise Risk Management Integrating with

Strategy and Performance framework (2017) remain the foundational reference points for internal audit's understanding of control and risk.

COSO Element	Audit of AI	AI in Audit
Control Environment		
Governance, Ethics & Accountability	Has the board articulated an AI governance policy? Are accountability structures for AI decisions clearly assigned? Is there genuine oversight of AI risk at the top? An organisation deploying AI without these structures has a deficient control environment, irrespective of technical sophistication.	The audit function must govern its own AI tools equivalently. Does the CAE have a policy on tool selection, validation, and use? Accountability for tool performance must be assigned. The function cannot credibly audit the organisation's AI governance without demonstrating the same standard internally.
Risk Assessment		
AI-Specific Risk Categories	Has the organisation's risk assessment been updated to include model risk, data risk, algorithmic drift and explainability risk? Are risk responses proportionate and within the stated risk appetite?	Has risk-based audit planning been updated to treat AI systems as a distinct risk category? When deploying AI audit tools, the risk of unreliable outputs must be assessed and compensated for through complementary procedures.
Control Activities		
Policies, Procedures & Controls	Examine controls over model development, validation independence, data quality, access to model parameters, change management, human override mechanisms, and output monitoring. The existence of a validation function alone is insufficient — assess its independence, rigour and whether its findings are acted upon.	Establish controls over AI audit tools: documented validation before deployment, access controls over audit data, change management for tool updates, and review protocols for AI-generated outputs before incorporation into working papers. Subject these controls to the quality assurance programme
Information and Communication		
Data Quality & Disclosure of Limitations	Are AI inputs complete, accurate and timely? Are outputs communicated with their limitations confidence intervals, known biases and model boundaries clearly disclosed to decision-makers? An AI output without disclosed limitations is a communication failure and a reportable control deficiency.	Working papers must document not only what the AI tool found but also its limitations and the auditor's independent evaluation of its outputs. Reports to the audit committee should distinguish clearly between AI-generated findings and the auditor's own conclusions.

COSO Element	Audit of AI	AI in Audit
Monitoring Activities		
Ongoing & Separate Evaluations	Are model performance metrics tracked against baselines? Do deviations trigger investigation and remediation? Is monitoring independent of model developers? Note the convergence: AI-enabled continuous auditing tools contribute to this layer, simultaneously discharging a COSO monitoring obligation and demonstrating AI in audit	The quality assurance programme constitutes the function's monitoring of its own AI tools. Review tool performance periodically; compare AI-generated findings against auditor-identified findings; investigate any tool failure promptly. Report results to the CAE on a defined cycle.
ERM — Strategic Dimension		
Risk Appetite & Strategy Alignment	Are AI risks reflected in the enterprise risk profile and reported to the board? Does the risk appetite statement address AI exposures? An AI strategy unaccompanied by an AI risk strategy is an incomplete — and reportable — strategic decision.	The function's AI tool deployment is itself a strategic decision. The CAE should assess the risk of tool failure — including reputational risk from deficient AI-assisted work — and ensure tool governance is commensurate with that risk.

In sum, the COSO frameworks do not need to be set aside when auditing AI. They need to be applied with heightened attention to the specific risk categories and control requirements that AI introduces. A recognised limitation arises when AI models function as inherently opaque deep learning systems whose internal mechanisms remain inaccessible even to their developers. In such cases, COSO's control activities framework should be augmented with outcome-based testing and explainability evaluation. An internal auditor well-versed in both COSO and AI will discover that their terminologies complement each other more than expected, but should not presume that expertise in one automatically translates to proficiency in the other.

Why This Matters and How It Helps: Direct inquiries from Audit Committees regarding AI testing require precise, technical responses. Internal audit departments will now have to retune their approach and upskill to ensure the expectations are met.

The audit universe changes: Clarity on the two dimensions means AI systems are treated as distinct audit subjects with their own risk ratings and not subsumed within general IT audit. The annual plan carries discrete AI engagements with specific objectives including model validation independence, training data representativeness, algorithmic drift, human override controls, and board reporting accuracy. "Reviewing AI controls" is not an audit objective.

Coverage expands materially: AI-enabled tools within the function permit full-population testing rather than sampling, continuous monitoring in near-real time, and NLP-assisted review of governance documentation. These are not incremental improvements; they represent a qualitative shift in what the function can observe and report.

Automation bias is the primary discipline risk. The tendency to treat the absence of an AI alert as assurance is among the most insidious risks the function faces. Mitigation requires deliberate controls: mandatory independent review of AI-generated findings before inclusion in working papers, periodic comparison of tool outputs against manually identified findings, and explicit training that builds auditor familiarity with each tool's known blind spots. AI-generated outputs are inputs to professional judgement and not

its replacement. The audit opinion remains the considered conclusion of a qualified professional, formed on evidence evaluated with scepticism.

The regulatory direction is unambiguous. India's DPDPA 2023 is in force. RBI and SEBI have issued related guidance carrying supervisory weight. Explicit obligations, mandatory disclosure, and direct accountability for AI failures are expected. The function that waits for regulation to arrive before building AI capability will find itself permanently behind the standard its organisation is required to meet.

Responsibilities of the Board, Audit Committee, Risk Management Committee, and the Executive Management:

The Board bears ultimate accountability for AI strategy and risk appetite, including approving an AI governance policy and ethical AI principles under the Companies Act, 2013, and Corporate Governance requirements.

The Audit Committee must ensure that AI systems affecting financial reporting are subject to adequate controls and independent validation, and that the internal audit function possesses the technical competence to audit them.

The Risk Management Committee must ensure that model risk, algorithmic drift, third-party AI vendor risk, and AI-related cybersecurity exposure are formally captured in the risk register with defined risk responses.

At the executive management level, AI governance is similarly distributed to the C-Suite Officers who carry distinct accountabilities that internal audit must understand, engage with appropriately, and audit independently applying the Three Lines Model consistently in each relationship.

Internal audit coordinates with, and provides assurance input to, all the above whilst remaining independent from each.

The Internal Audit AI Maturity Model: Where the Function Stands and Where It Must Go

Competence in both dimensions of AI practice i.e., using AI within the audit function and auditing AI systems within the organisation does not arrive fully formed. It develops along a discernible progression. The framework below maps that progression across four stages, addressing both dimensions in parallel. It is a diagnostic and a structured means of identifying the gap between where the function stands and where its professional obligations require it to be.

Stage	Maturity Level	IA Using AI	AI Subject to IA
Stage 1	Initial Unaware — obligation not yet recognised	Audit work is conducted manually or with basic spreadsheet tools. Data analytics, if used, are ad hoc. AI tools have not been formally evaluated, procured, or governed.	AI systems within the organisation's operations have not been identified as a distinct category of audit subject. AI-related risks do not appear as a separate line in the audit universe. If AI systems are reviewed at all, they are treated as a subset of general IT audit without specialist methodology.
Stage 2	Developing Aware — action tentative and inconsistent	Basic data analytics and robotic process automation are being deployed in selected engagements. Usage depends on individual auditor capability rather than function-wide standards. Governance of tools is informal.	AI-related risks have begun appearing in the audit universe, but coverage is minimum. The IA Head is aware of the obligation but has not yet invested in the specialist competence which is essential.
Stage 3	Established Capable — methodology embedded, coverage consistent	AI tools are embedded in standard audit procedures including continuous monitoring, full-population testing, review of contracts and board minutes. Automation bias is actively managed.	The function conducts structured AI audit engagements using a defined methodology. Audit objectives cover model validation independence, training data quality, human override controls, algorithmic drift monitoring, and board reporting accuracy. Findings are reported to the Audit Committee with appropriate technical rigour.
Stage 4	Optimising Leading — continuously improving on both dimensions	The function's AI capabilities are subject to continuous evaluation and improvement. New tools are assessed against a defined governance framework before deployment. The quality assurance and improvement programme explicitly covers AI tool performance. The IA Head reports periodically to the Audit Committee on the function's AI tool usage, limitations, and governance.	The function is a technically credible voice in the organisation's AI governance discussions. It contributes to board-level understanding of AI risk without compromising its independence.

The Three Investments Required to Advance

1. Technical Capability
Recruit data scientists and AI specialists into the function or build structured relationships with specialist advisors whose independence from the systems being audited can be assured. Generic data analytics skills are necessary but not sufficient for Stage 3 and beyond.

2. Methodology
Adopt and adapt established frameworks viz., COSO, IIA GTAG guidance on data analytics, and IIA's emerging AI auditing standards rather than approaching each AI engagement from first principles. Consistency of methodology is what makes findings comparable and credible.

3. Governance of Own Tools
Apply to the function's own AI tools the same validation, monitoring, and documentation standards the function would treat as non-negotiable in the organisation. The internal auditor cannot credibly assess what it does not demonstrably practise.

The Human Capital Imperative

The three investments above assume that the people required to make them are available. That assumption cannot be taken for granted. Data scientists, AI specialists, and professionals who combine technical AI competence with audit methodology are among the most competed-for resources in the current talent market. The IA who understands the constraints, plan their actions around it by building structured relationships with specialist advisors whose independence from audited systems is contractually assured, negotiating co-sourcing arrangements with firms that bring AI audit capability the function does not possess internally and investing in the technical literacy of the existing audit team through targeted development. The single variable that most consistently determines whether a function advances from Stage 2 to Stage 3 of the maturity model is not budget or technology; it is the IA's own technical literacy.

AI in Practice

How the Audit Engagement Actually Changes: When AI is both the subject of audit and the instrument of audit, the engagement must be conducted differently at every stage.

At the planning stage, each material AI model demands its own risk rating and its own audit objectives and not subsumption within general IT audit. The auditor must map the organisation's AI landscape before scoping begins. Where the organisation cannot produce a complete, current model inventory, that gap is itself the first reportable finding.

During fieldwork, AI-enabled tools transform coverage from sampled to complete, every transaction, journal entry, and contract clause becomes testable. But the auditor must document not merely what the tool found, but what it was not designed to find. The tool's scope is simultaneously its strength and its limitation. The auditor who does not understand what the tool cannot see will not notice what it has missed.

At the reporting stage, the distinction between an AI-generated output and the auditor's independent conclusion must be unambiguous. A finding surfaced by a tool is not the same as a finding reached by professional judgement, even when both arrive at the same place. The audit opinion is always the latter. A committee that cannot tell which findings came from a tool and which from the auditor cannot properly evaluate the assurance it is receiving.

Issues that consistently arise and are rarely anticipated:

- The model being run is not the model that was validated. Parameter changes, retraining events, and vendor updates accumulate silently between audit cycles. Validation at a point in time is not durable — and treating it as such is among the most common and consequential AI audit failures.

- Shadow AI is almost always present. Business units adopt AI tools through software subscriptions outside formal governance. These systems influence decisions whilst remaining invisible to an auditor relying solely on the declared register.

- The vendor assurance report answers the wrong questions. SOC 2 reports address operational controls and not model accuracy, fairness, or fitness for purpose. The auditor must read the scope before placing any reliance.

- Technical findings not translated into business consequence are not acted upon. Discovery of facts or analysis of the data is only the starting point using AI, the further action on its impact and the corrective action that may be required and designed to the circumstances should drive the departments for action.

The Stakeholder Dimension: Who Bears the Consequences

AI governance is not an internal professional matter. When it fails and when internal audit fails to catch that failure, the consequences fall on people and institutions well beyond the boardroom.

- **Customers:** An AI model making credit, insurance, or service decisions may be biased, miscalibrated, or operating outside its validated parameters and customers will rarely know. For technology service providers, SOC 2 reporting addresses operational controls but says nothing about model fairness or output accuracy. IA, deploying statistical bias-testing tools across the full population of AI-assisted customer decisions, can detect discriminatory patterns that sampling would never surface and report them before they become regulatory or reputational events.

- **Employees:** AI is increasingly used in recruitment screening, performance evaluation, and workforce planning. Employees subject to these decisions have a legitimate interest in fairness, explainability, and human review. IA using algorithmic fairness testing tools can analyse HR model outputs across demographic cohorts, identifying bias encoded in the model that neither HR nor management has visibility of and that no manual audit process could efficiently detect.

- **Vendors and Third Parties:** The vendor's model becomes the organisation's risk. Assurance reports provided by vendors rarely cover model accuracy, fairness, or fitness for purpose — and where the model is proprietary, the vendor may resist access entirely, citing intellectual property. IA using automated contract analysis tools can systematically assess whether vendor agreements preserve audit rights and whether vendor-provided assurance matches the risks the organisation actually carries. Where access is denied, that limitation is itself a reportable finding.

- **Shareholders and Investors:** AI governance failures manifest in financial statements through restatements, penalties, and litigation. ESG-focused investors treat AI governance as a proxy for management quality. IA using continuous monitoring tools provides shareholders and investors with something no disclosure document can: independent, evidence-based assurance that AI governance is substantive not merely reported as such.

- **Regulators:** Regulators are tightening AI obligations across every supervised sector. IA that identifies governance failures before the regulator does is the organisation's most valuable early warning system. IA using AI-powered regulatory change monitoring and compliance gap analysis tools ensures the organisation's AI framework keeps pace with evolving requirements rather than discovering the gap when the inspection arrives.

- **Community and Society:** AI deployed at scale in public services, lending, healthcare, and infrastructure shapes outcomes for communities with no direct voice in how those systems are governed. IA is the only independent function routinely positioned to assess whether these systems are operating as intended. AI-enabled audit tools including testing model outputs at population scale, detecting drift, and assessing explainability give IA the reach to discharge that obligation meaningfully, rather than symbolically.

The Cybersecurity Dimension

AI introduces attack which are far different from the conventional ones including adversarial manipulation of model inputs, poisoning of training datasets, and model inversion attacks that extract sensitive personal data from trained models. Internal audit must assess whether cybersecurity controls extend explicitly to AI assets and not merely to traditional systems. AI simultaneously strengthens

and threatens cybersecurity. AI-powered threat detection is faster and more comprehensive than rule-based systems including, use of AI to generate convincing phishing, automate vulnerability scanning, and produce deepfakes for social engineering.

The RBI's Cybersecurity Framework (updated 2023) and SEBI's Cybersecurity and Cyber Resilience Framework (2023) require controls over AI assets specifically; internal audit in regulated entities must include AI-specific cybersecurity objectives in its audit universe. The same rigour applies inward i.e., the IA's own AI tools process sensitive organisational data and must be subject to equivalent controls including access controls, encryption, secure transmission, and vendor security assessments as minimum requirements.

The Generative AI Dimension:

Large language models and generative AI tools represent a distinct and rapidly expanding category of AI risk that warrants explicit treatment. Most internal auditors will encounter generative AI, because their own organisations are deploying it, and because the audit function itself is using it. As an audit subject, generative AI presents risks that differ materially from those of conventional predictive models including outputs are probabilistic rather than deterministic, meaning the same input can produce different outputs; hallucination i.e., the confident generation of factually incorrect content is an inherent characteristic rather than a defect; training data may incorporate copyrighted material or personal data without adequate disclosure; and the explainability of any specific output is, in most architectures, not achievable in a meaningful sense.

Internal audit must assess whether the organisation has identified all generative AI deployments, whether human review is mandatory before AI-generated content is used in consequential decisions or external communications, and whether the confidentiality of prompts which frequently contain sensitive organisational or personal data is protected. As a tool within the audit function, generative AI used for working paper drafting, findings summarisation, or report generation must be governed with the same rigour: outputs verified before use, limitations documented, and the auditor's independent judgement applied to everything the tool produces. The function that uses a large language model to draft audit findings without verifying their factual accuracy has introduced precisely the kind of ungoverned AI risk it is obliged to audit in others.

Emerging Dimensions: What the Profession Must Confront Next

- **Ethical Dilemmas:** AI sharpens the internal auditor's ethical obligations into something more demanding than any prior era has required. When an AI system produces an outcome that is technically compliant but causes demonstrable harm, documenting the control may not be sufficient and professional ethics may require the auditor to say so explicitly. When the audit function's own tool produces a finding the auditor doubts, choosing between the algorithm and one's own judgement is an ethical decision, not merely a technical one. When an organisation deploys AI faster than its governance framework can support, the CAE's obligation to report that gap even when leadership is unreceptive, tests independence in a way that conventional audit rarely does.

- **Skill Evolution:** Data literacy is now a baseline expectation, not a specialist skill. Beyond it, the AI-era auditor needs working familiarity with model validation, statistical bias testing, prompt engineering, and sector-specific AI regulation. More importantly, AI capabilities are evolving faster than any curriculum can track. Continuous learning including structured, disciplined, and verifiable is itself now an audit competency.

- **AI Explainability and Trust:** An AI-generated finding the auditor cannot explain to management is not a finding, it is a hypothesis. Trust in AI systems is earned through demonstrated accuracy and transparency about limitations and lost immediately when those properties fail. Providing independent assurance that AI systems perform as represented is one of the most valuable services internal audit can offer.

- **Future Scenarios:** Autonomous audit agents capable of conducting end-to-end procedures with minimal human intervention are already in early deployment. The question of what professional responsibility attaches to autonomously generated findings will require the profession to revisit its standards fundamentally. More immediately, auditing AI will cease to be a specialist engagement and become a routine component of every audit programme.

Conclusion:

The emergence of AI presents the internal audit profession with its most rigorous test yet not because AI is incomprehensible, but because it operates simultaneously on both sides of the audit equation. The COSO and ERM frameworks provide the structured vocabulary to examine both dimensions rigorously: assurance over the organisation's AI systems on one side; disciplined, well-governed use of AI tools within the audit function on the other.

The internal auditor who holds both perspectives with equal clarity bringing professional scepticism to AI outputs whether they originate in the organisation or in the audit function itself is the auditor this era demands. The consequences of not doing so extend beyond professional shortfall: they fall on customers subjected to biased decisions, employees assessed by ungoverned algorithms, communities served by AI systems that no one has independently examined, and shareholders whose capital is exposed to risks that management reporting does not surface.

The old verities of the profession i.e., independence, objectivity, professional scepticism, ethical commitment are as essential as they have ever been, and in the AI era they acquire new content. Independence is tested when the function audits systems it also uses. Objectivity is tested when AI tools confirm what the auditor already suspects.

Professional scepticism is tested when the AI produces no alert and the auditor is tempted to conclude there is nothing to find. And ethical commitment now includes an obligation the profession has not previously had to articulate explicitly: the obligation to consider whether an AI system, even if technically compliant and adequately controlled, is causing harm to people who have no voice in how it operates. Artificial intelligence is an immensely powerful tool.

The internal auditor remains the professional. That distinction, clearly held and actively lived, is the foundation upon which effective practice in the AI era must be built.

The Institute of
Internal Auditors
India | Calcutta Chapter

The Institute of Internal Auditors India – Calcutta Chapter

JOINT AUDIT CONCLAVE

FOR THE MEMBERS OF

ICAI | ICMAI | ICSI | ISACA

THEME

IA: TRUST, TECHNOLOGY & TRANSFORMATIVE GOVERNANCE

SUB THEME

Redefining IA-AI as Strategic Compass

DATE
19 JUNE 2026
FRIDAY

VENUE
NOVOTEL
KOLKATA

WHO SHOULD ATTEND
Chief Audit Executives
Internal Auditors
Risk & Compliance Professionals
CXOs | Governance Professionals
Academia | Students

SECURE YOUR SPOT TODAY
SCAN TO REGISTER

COLLABORATE • INNOVATE • TRANSFORM

SHAPING THE FUTURE OF ASSURANCE

Strengthening Digital Trust

The Expanding Role of Internal uditors in Digital Data Protection - Banking and Financial Services

Snapshot

India's Digital Personal Data Protection (DPDP) Act, 2023 and the Digital Personal Data Protection Rules, 2025 mark a major shift in how organizations collect, store, and process personal data.

This series of articles explore the evolving role of internal auditors across major sensitive industries, explains their key risk areas and highlights internal auditors' responsibilities with reference to the DPDP provisions as well as Standards on Internal Audit issued by ICAI in February, 2026. The DPDP law has re-shaped the scope of internal auditors in a manifold way - creating both opportunities and challenges.

Internal Auditors' Understanding of what makes Data "Sensitive" and their evolving role

The DPDP Act does not provide a fixed list of "sensitive personal data." Instead, the level of risk is determined by context - how much harm could result if that data is misused, leaked or mishandled.

Internal auditors must evaluate security systems, lawful processing, and proactive privacy risk management.

Greater emphasis on Standard on Internal Audit (SIA) 160 - Compliance with Laws and Regulations shall be the key in understanding the industry specific scope and SIA 150 - Risk Management shall be the key to assess the risk involved in that particular industry. The auditor's role shall be to evaluate the design of risk management framework within the DPDP environment for an entity.

Banking and Financial Services Sector : Board Responsibilities and evolving role of their internal auditors

Banks and financial institutions process highly sensitive data - names, identification numbers, account details, transaction records, and biometric authentication. This makes them one of the most vulnerable industries under the DPDP framework.

The key risks include :

- unauthorized sharing of customer data with third parties,
- inadequate consent management for digital lending and
- data retention beyond required periods.

mita Nikhil Kavle
IC I (The Institute of Chartered ccountants of India)
Head - ccounts and Finance at WIRC of IC I

A consolidation of specific data protection measures that a banking company (disbursing loans) will need to build in their data bases and a checklist that auditors need to check during their internal audit is shown in the table below :

Internal Control to be set up by Bank (Housing Loan Service Provider)	Detailed checklist that auditors will have to build with Reference to DPDP Act / Rules and with Reference to Standards on Internal Audit (SIAs)
Data Collection for sanction and disbursal of loan : • The Bank must collect only essential information from prospective customers like : name, address, contact details, Income tax return copies, income proofs, KYC documents like government identity cards, Property details and related documents for purchase and sale transaction like sales deed/ agreement, bank account details in which loan is to be disbursed etc. - all which are mandatorily required as per the home loan sanction and home loan disbursal process of the bank. • No irrelevant customer data should be captured in the systems of the bank which is not relevant in providing the home loan services. **Data Storage with 'Verifiable Consent'** • Banks must maintain accurate data systems to capture only data required for home loan sanction and disbursal.	**Section 2 (za)** - applicable for collection of data for specified purpose only **Standard on Internal Audit (SIA) 210 - Knowledge of the Entity and it's Environment** - in determining the legitimate purpose at first place. **SIA - 250 on Internal Audit Documentation, especially para 4.2 :** Content and sufficiency of Documentation **Here the auditors will have to :** • Understand the bank's operations, governance structure, and home loan processes to evaluate the auditee bank's risk management framework. • Document the role of internal teams such as IT, Business Development, Legal, and Finance in designing and managing data systems. • Review and document the bank's customer consent mechanism, including system process flow and backend data capture. • Evaluate the bank's policy on consent and data processing to ensure only lawful and relevant data is collected for home loan services. • Conduct sample checks of physical and electronic customer files to verify the nature of data collected and stored in digital systems. • Verify the accuracy of data collected and stored for processing. • Review the internal flow of customer data across departments and assess the purpose of such movement **Compliance as per Section 2(d) of the DPDP Act ie. verifiable consent as mentioned in Rules 10 and 11 of the Rules)**

Internal Control to be set up by Bank (Housing Loan Service Provider)	Detailed checklist that auditors will have to build with Reference to DPDP Act / Rules and with Reference to Standards on Internal Audit (SIAs)
• Banks should establish verifiable consent mechanisms allowing customers to separately consent for home loan processing and for marketing or ancillary purposes. • Customers should be able to easily provide or withdraw consent through simple and accessible mechanisms.	**Standard on Internal Audit (SIA) 230** **Internal Audit Evidence - for arriving at conclusions which form the basis of audit report.** **Here the auditors will have to:** • Check whether the bank obtains separate and free customer consents for home loan services and for marketing or ancillary purposes. • Review sample customer records to verify that mechanisms such as designated emails or online portals are available for withdrawal of consent, and ensure such requests received physically or electronically are properly documented and implemented on time. • Verify backend IT logs to assess how consent-related requests are received, processed, and disposed of to ensure compliance and prevent breaches of law.
Data Safeguards : • Banks should maintain regular backups of customer data at secure locations with encryption, masking, and restricted access controls to prevent unauthorized access. • Banks should establish controls to monitor and update customer data whenever changes are initiated by the data principal.	***Standard on Internal Audit (SIA) 270 - Experts and Third-Party Engagement*** *(For Relying on the Work of Data Processing officer for Data Protection Impact Assessment)* ***Standard on Internal Audit (SIA) 270 - Experts and Third-Party Engagement*** (For Relying on the Work of Data Processing officer for Data Protection Impact Assessment) **Here the auditors will have to :** • Auditors should verify that adequate backup policies, regular backups, and audit logs are maintained by the bank. • Auditors should ensure that data access is restricted to authorized staff based on their roles and hierarchy levels, with proper segregation of duties and data masking controls to prevent unauthorized access or leakage. **Example 1 :** KYC teams should have access only to Digital Locker documents. **Example 2 :** Home loan staff should not access unrelated customer information such as car loan or insurance details. • Auditors should verify IT controls restricting external

Internal Control to be set up by Bank (Housing Loan Service Provider)	Detailed checklist that auditors will have to build with Reference to DPDP Act / Rules and with Reference to Standards on Internal Audit (SIAs)
	storage devices, personal emails, and unauthorized application downloads on organizational systems. • Auditors should ensure that personal data is not improperly shared with vendors, subcontractors, or fintech partners, and that adequate contractual safeguards exist wherever sharing is necessary. • Internal auditors may rely on the work of the Data Protection Officer, with such reliance and audit evidence properly documented. • Auditors should ensure that DPDP compliance responsibilities are assigned to internal officers and those charged with governance (TCWG).
Data erasure policy and implementation : • Banks should maintain policies and controls defining when customer data is no longer required, including after loan closure and settlement. • Periodic assessments should be conducted by the DPIO or authorized personnel to ensure data deletion complies with applicable rules and proper notice is issued to customers. • Banks should maintain systems to monitor, report, and timely address data breach incidents.	**Compliance in accordance with Section 12(1), (2) and (3) - Right to correction and erasure of personal data :** **Here the auditors will have to :** • Auditors should verify that, upon loan closure, banks proactively initiate customer data erasure requests, especially for high-value transactions. In the absence of customer response within the prescribed period, data should be erased with due notice to the customer. • Auditors should test check high-value transactions to ensure complete and not selective erasure of customer data from the bank's systems.

Road Ahead for Internal Auditors

The DPDP Act represents more than a compliance requirement — it reflects a mindset shift. Internal auditors are evolving into 'Data Privacy Guardians', with a growing focus on proactive audits and cross-functional collaboration with IT, Legal, and ESG professionals.

II India Bombay Chapter

IIA Bombay Chapter Celebrates Internal Audit Awareness Month

As part of its continued commitment to advancing the internal audit profession and fostering stronger industry engagement, the IIA Bombay Chapter commemorated Internal Audit Awareness Month through a series of engaging initiatives aimed at promoting collaboration, professional excellence, and community building within the fraternity.

A key highlight of the celebrations was the successful hosting of the Internal Audit Premier League (IAPL) on 30th May 2026, which brought together professionals from across the corporate ecosystem for a spirited day of cricket, networking, and camaraderie.

The tournament witnessed enthusiastic participation from 15 teams representing leading organisations across industries. The event reflected the shared values of teamwork, resilience, discipline, and leadership that are integral to the internal audit profession.

Beyond the excitement on the field, the initiative created a vibrant platform for meaningful interaction and relationship-building beyond conventional professional settings. The exceptional sportsmanship and collaborative spirit displayed throughout the event further reinforced the growing sense of community within the internal audit fraternity.

Through such initiatives, the IIA Bombay Chapter continues to strengthen awareness around the profession while encouraging engagement, wellness, and stronger industry connections.

The Chapter extends its sincere appreciation to all participating organisations, players, partners, and supporters for contributing to the success of the celebrations.

4th April – Audi Committee Expectations from Internal Audit: Delivering Insight, Assurance & Value

The Institute of Internal Auditors (IIA) India – Bombay Chapter successfully conducted an insightful webinar on "Audit Committee Expectations from Internal Audit: Delivering Insight, Assurance & Value" on 4th April 2026, featuring Mr. Ravi Varma, Company Secretary, Emami Limited.

The session witnessed an overwhelming response with around 177 registrations, reflecting the growing interest among professionals in strengthening governance, strategic assurance, and value-driven internal audit practices. Participants appreciated the practical insights shared on emerging risks, technology-driven auditing, impactful reporting, and the evolving expectations of Audit Committees from Internal Auditors. The webinar provided valuable learning opportunities and encouraged meaningful discussions on how internal audit can move beyond compliance to become a strategic business partner.

Awards Partner: LASER
Merchandise Partner: Protiviti

18th April – Designing Effective Audit Programs: A Risk -Focused and Value Driven Approach

The Institute of Internal Auditors (IIA) India – Bombay Chapter successfully organized an engaging webinar on "Designing Effective Audit Programs: A Risk-Focused and Value-Driven Approach" on 18th April 2026, led by Dr. Satish Kumar Gupta, Head of Internal Audit, Berar Finance Limited.

The webinar received an excellent response with approximately 172 registrations, highlighting the keen interest of audit professionals in developing impactful and strategic audit methodologies. The session focused on designing audit programs that prioritize high-risk areas, align with organizational objectives, and deliver meaningful business insights beyond traditional compliance reviews.

Participants highly appreciated the practical perspectives shared on dynamic risk assessment, value-driven

auditing, and enhancing audit efficiency through smarter planning and focused execution. The webinar served as a valuable platform for professionals to strengthen their understanding of modern internal audit practices in an evolving business environment.

16th May – Writing Impactful Internal Audit Reports: from findings to actional Insights

The Institute of Internal Auditors (IIA) India – Bombay Chapter conducted a highly informative webinar on "Writing Impactful Internal Audit Reports: From Findings to Actionable Insights" on 16th May 2026, featuring Mr. Hitesh Khandhadia, Associate Director, V C Shah & Co.

The webinar attracted an excellent participation with around 184 registrations, demonstrating the strong interest among professionals in enhancing audit communication and reporting effectiveness. The session focused on transforming audit observations into meaningful, actionable insights that support better decision-making and stakeholder engagement. Participants gained practical guidance on drafting clear, concise, and persuasive audit reports, improving presentation skills, and adopting best practices for impactful audit communication. The webinar was widely appreciated for its practical relevance and valuable insights into strengthening the overall effectiveness of internal audit reporting.

Internal Audit Compliance Series - 2026

The Institute of Internal Auditors (IIA) India – Bombay Chapter, jointly with the Western India Regional Council of ICAI, is conducting the "Internal Audit Compliance Series – 2026", a 10-day virtual learning series from 22nd May 2026 to 24th July 2026.

The series covers key compliance and regulatory areas including Labour Laws, RBI Risk Based Audit, DPDP, IT Act & AI Governance, SEBI Compliance, Companies Act, GST, Income Tax, Ind AS, FEMA, IBC, and PMLA/AML. Sessions are led by eminent speakers and aim to provide practical insights into emerging compliance requirements and risk-focused internal audit practices.

The initiative has received an encouraging response from professionals across the audit and finance fraternity, reflecting the increasing importance of compliance-driven assurance and governance.

CIA Challenge Exam Coaching Class

The Institute of Internal Auditors (IIA) India – Bombay Chapter has commenced the CIA Challenge Exam Prep Course – 2026, a specialized weekend coaching program designed to support professionals preparing

for the CIA Challenge Exam. The sessions started on 23rd May 2026 and are being conducted on weekends from 7:00 AM to 10:30 AM.

The program focuses on conceptual clarity, exam-oriented MCQ practice, revision sessions, query resolution support, and access to Gleim study materials, helping participants strengthen their preparation through a structured and practical learning approach. The initiative has received an encouraging response from aspiring CIA professionals aiming to fast-track their certification journey.

20th May - CAE Roundtable for banks | 27th May - CAE Roundtable for NBFC

In the lead-up to the 6th Annual BFSI Conclave, scheduled to be held in Mumbai on 5 June 2026, the IIA Bombay Chapter convened two distinguished Chief Audit Executive (CAE) Roundtables, bringing together senior internal audit leaders from across India's banking and financial services landscape.

The first roundtable, held on **20 May 2026** and hosted by **Kotak Mahindra Bank,** witnessed the participation of 30+ CAEs and senior leaders representing many of the country's leading banks. The session provided a valuable forum for deliberating on the **evolving risk landscape, emerging governance imperatives, and the transformative role of internal audit** in an increasingly dynamic financial ecosystem. Neurofin AI partnered the event.

The second roundtable, hosted by **L&T Finance on 27 May 2026,** brought together 40+ CAEs from across the BFSI sector. Discussions centred on contemporary challenges, emerging opportunities, and strategic priorities shaping the future of the internal audit profession. The event was supported by Kirtane & Pandit and Neurifin AI.

Collectively, the two roundtables fostered **insightful dialogue**, facilitated the **exchange of perspectives and leading practices,** and strengthened professional collaboration among audit leaders. The deliberations served as a fitting prelude to the **6th Annual BFSI Conclave,** underscoring the profession's continued commitment to **excellence, innovation, and resilient governance.**

Reimagining Audit Methodology in a Full-Population Testing World

For decades, internal audit methodologies have been built around one foundational principle: sampling. Auditors selected representative transactions, tested controls over those samples, and formed conclusions on the effectiveness of the broader process. The model was practical and aligned to an era when extracting and analyzing large volumes of data was both difficult and time consuming.

That environment no longer exists.
In a recent Audit Committee discussion at a large organization, the Chairman posed a pointed question to the internal audit team: "If the systems today process every transaction digitally, why are auditors still giving assurance based on 25 or 30 samples?" In another discussion around analytics and AI adoption, a board member questioned why internal audit continued to perform limited testing when technology now allowed entire populations to be reviewed.

These are no longer isolated questions. They reflect a broader shift in stakeholder expectations.

Today, organizations operate through integrated ERP platforms, automated workflows, and centralized shared service models that generate millions of data points every day. In such an environment, the question facing internal audit is no longer whether enough samples have been tested, but whether the audit function is interpreting the right signals from the data available to it.

The move toward full-population testing is therefore not simply a technology upgrade. It is forcing a fundamental rethink of audit methodology itself.

From Sampling Cop to Pattern Detective

Traditional audits were designed around limitations in technology and access to data. Sampling helped auditors obtain reasonable assurance without reviewing entire transaction populations.

With modern analytics tools, however, organizations can now scan complete datasets across processes such as procure-to-pay, payroll, journal entries, inventory management, and user access administration. Automated rules can identify duplicate payments, unusual transactions, approval overrides, or segregation-of-duties conflicts across the entire population rather than a limited sample.

Technology is what enables this shift. ERP data lakes, visualization platforms, automated scripts, AI-assisted anomaly detection, and continuous monitoring routines now allow auditors to evaluate trends and exceptions at a scale that was previously impractical. Instead of manually selecting

Manish Tibrewal
Manager – Finance Modernisation
Major BFSI GCC - Leader in Global Services

transactions for testing, auditors can configure logic that continuously scans for risk indicators across millions of records.

This changes the role of the auditor significantly.

Internal audit's value no longer lies in how much it tested, but in how intelligently it interrogates data. The auditor's instinct—what "feels wrong" in a process—must increasingly be translated into anomaly rules, query logic, and risk indicators.

In effect, human judgment moves upstream. Auditors are no longer spending most of their time deciding which transactions to test; they are defining what patterns, behaviors, or exceptions deserve attention in the first place.

The shift is subtle but profound: auditors move from being "sampling cops" to becoming "pattern detectives."

The "So What" Problem

While full-population testing increases visibility, it also introduces a new challenge: data overload.

In many organizations, initial analytics exercises generate thousands of exceptions. Without a structured methodology to interpret these outputs, audit teams risk producing reports that are little more than exception dumps.

This is where audit rigor becomes critical.

Internal audit functions must develop clear triage frameworks that distinguish noise from meaningful risk signals. A single isolated exception may not matter. A recurring pattern across locations, users, vendors, or business units may indicate something far more significant.

For example, in a large Indian manufacturing or retail organization operating through centralized finance teams, analytics may identify hundreds of manual journal entries posted after business hours. Individually, many may appear harmless. However, clustered patterns linked to specific users, reporting periods, or approval overrides may reveal deeper process or governance concerns.

The real value of full-population testing lies not in identifying more exceptions, but in identifying the exceptions that matter.

When Control Testing Gets Uncomfortable

The rise of full-population testing also raises uncomfortable questions about traditional control reliance models.

Historically, audits focused on evaluating whether key controls operated effectively during a defined period. But if technology allows auditors to analyze every transaction directly, the debate naturally

shifts: why rely solely on a preventive control when the actual outcomes can now be continuously evaluated?

This does not make controls irrelevant. Instead, it changes the focus of assurance.

Internal audit increasingly needs to evaluate process integrity rather than only output accuracy. Design weaknesses, override risks, inappropriate access combinations, and management intervention become more important areas of focus than merely validating transaction outputs through sampling.

For instance, in several GCC and shared services environments in India, automated workflows process extremely high transaction volumes with limited manual intervention. In such settings, a single override capability or poorly designed access role can create far greater risk exposure than isolated transactional errors.

As audit methodologies evolve, understanding how systems can be bypassed may become more important than simply confirming that transactions were processed correctly.

The Skills Gap Is the Real Risk

Technology itself is not the biggest challenge in adopting full-population testing. The larger risk is whether audit teams can interpret the data with sufficient audit rigor.

Many internal audit teams today can generate full-population extracts and build dashboards. Far fewer are equipped to translate analytics outputs into meaningful assurance conclusions.

Tools such as SQL, Python, Power BI, and visualization platforms are increasingly becoming baseline capabilities. However, the truly scarce skill remains the application of professional audit judgment to population-level data.

Training therefore needs to evolve as well. Audit functions must move beyond traditional sampling theory toward anomaly detection, pattern recognition, risk clustering, and data storytelling.

The future auditor will not only understand controls; they will understand how risk behaves within data.

Independence in a Real-Time Environment

As internal audit gains access to live operational data and real-time monitoring capabilities, maintaining independence and objectivity becomes increasingly important.

The closer audit gets to continuous monitoring, the easier it becomes for the line between assurance and management responsibility to blur. Internal audit must remain clear about its role: to observe, assess, and report—not to operate or optimize business processes.

This is particularly relevant as organizations establish continuous monitoring programs within ERP environments. Governance frameworks may need to evolve to ensure that full-population access and real-time visibility do not unintentionally compromise audit independence.

The Continuous Audit Opportunity

Full-population testing is not simply changing how audits are performed; it is reshaping what stakeholders expect from internal audit itself.

Boards and management teams increasingly expect assurance functions to provide timely insights into emerging risks rather than retrospective observations months after the event. Full-population testing enables internal audit to move from periodic assurance toward continuous risk sensing.

The question is no longer only "What happened last quarter?" but increasingly, "What is happening right now, and does it concern us?"

Ultimately, the future of audit methodology will not be defined by the size of samples tested, but by the ability of internal audit to convert vast amounts of transactional data into meaningful insight, timely escalation, and better governance outcomes.

The Institute of Internal Auditors
India - Delhi Branch

Annual Conference 2026

Audit Remagined:
Intelligence - Integrity - Impact

Date:
19th - 20th June, 2026

Time:
09:00 AM to 05:30 PM

Venue:
Holiday Inn, Aerocity, New Delhi

SAVE THE DATE

12 CPE HOURS

Contact us at:
delhibranch@iiaindia.co
coordination@iiaindia.co

Early-Bird Fees (Valid upto 31st May)
IIA Member: INR 9,000 + GST
Non-Member: INR 13,000 + GST

Regular Fees
IIA Member: INR 10,000 + GST
Non-Member: INR 15,000 + GST

II India Calcutta Chapter

BUILDING FUTURE-READYORGANIZATIONS
Balancing AI risks and opportunities

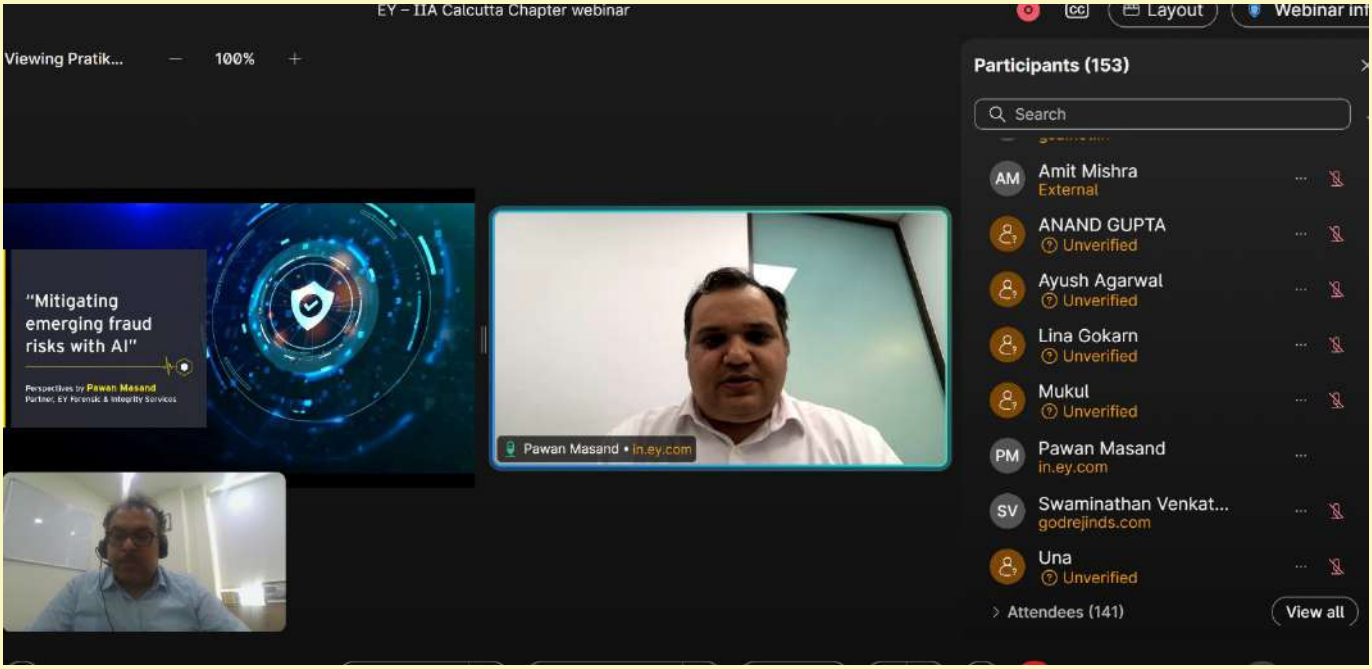
On May 8th 2026

The virtual session jointly hosted by EY and IIA Calcutta Chapter on "Building Future-Ready Organizations: Balancing AI Risks and Opportunities" brought together industry leaders, governance professionals and risk experts to deliberate on the evolving impact of AI on organizations.

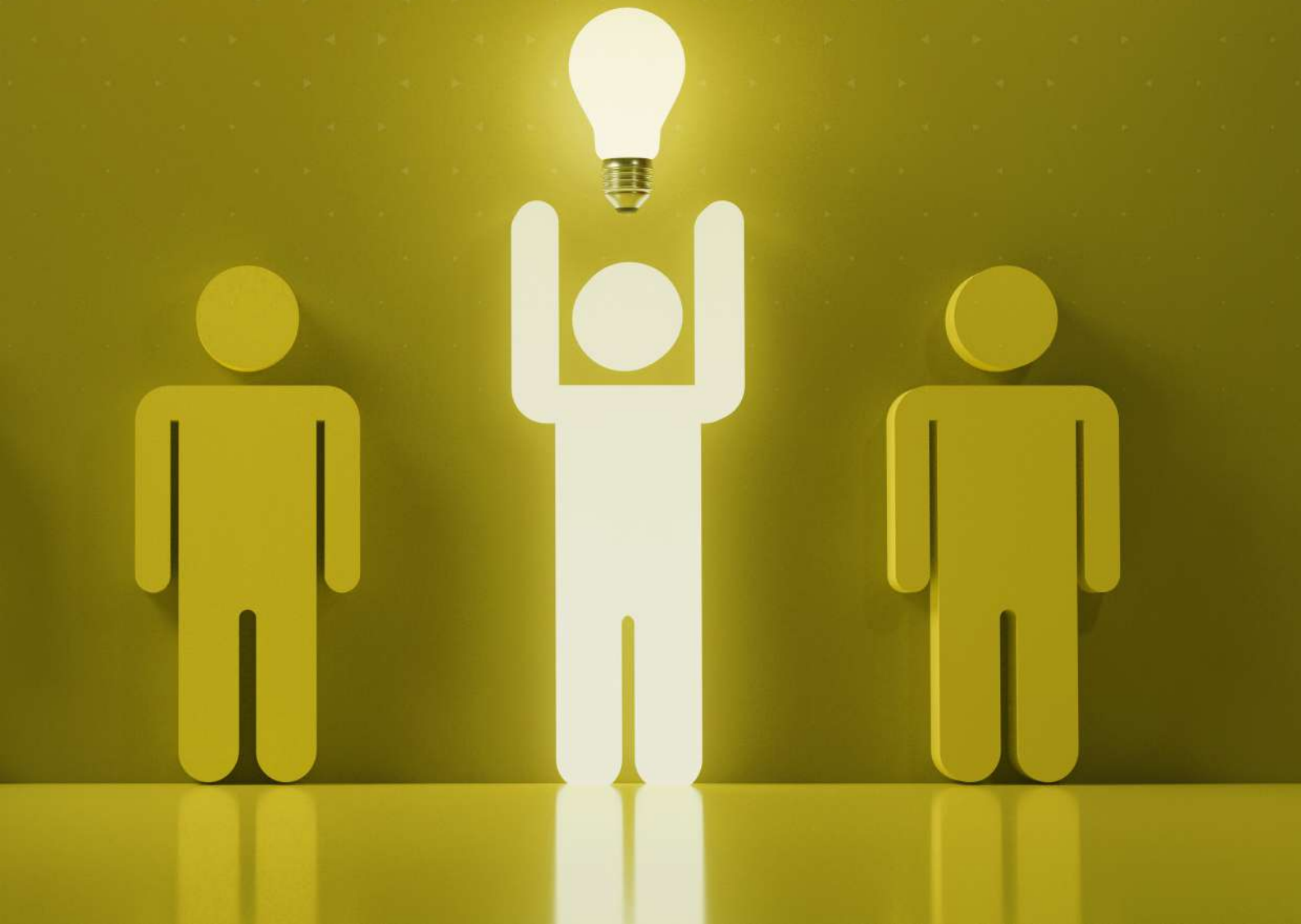
The session highlighted how AI is rapidly transforming business processes, while simultaneously creating new-age governance, fraud and compliance risks that organizations must proactively address. The event featured insightful keynote addresses and expert presentations from senior leaders of EY Forensic & Integrity Services, focusing on emerging fraud risks in an AI-driven environment.

A highly engaging panel discussion brought together distinguished leaders from industry and internal audit, including representatives from Tata Power, Godrej Group and EY, who shared practical perspectives on balancing innovation with resilience. The discussions emphasized the growing role of internal audit, ethics, governance and continuous risk monitoring in enabling responsible AI adoption.

The webinar witnessed active participation from professionals across sectors and concluded with an interactive Q&A session, reinforcing the importance of collaborative dialogue in shaping future-ready and risk-resilient organizations in the age of AI.



EMERGING MINDS STUDENT'S FORUM



The Third Line Reimagined

Internal udit in the ge of rtificial Intelligence

Aditya Kumar Jha & Vanya Singh
Scholar – Global Risk Management Institute(GRMI)

For decades, internal audit occupied a well-understood but quietly constrained role in the governance architecture of organisations. Its mandate — to provide independent, objective assurance and consulting — remained largely unchanged even as the business environment it surveyed grew exponentially more complex. Today, that equation is essentially disrupted. Artificial intelligence is not just offering internal audit a better toolkit; it is far stressing a wholesale consideration of what the feature is for, who it serves, and how it creates costs.

A Profession Built for a Slower World

The traditional internal audit model was essentially engineered for a world of periodic review. Audit plans were set annually. Fieldwork proceeded through structured walkthroughs, sample testing, and manual document review.

The structural weakness was not professional competence. It was the sheer mismatch between the velocity of modern risk and the cadence of traditional audit cycles. A financial institution processing millions of transactions daily cannot be meaningfully protected by an audit function that samples three hundred of them every quarter. A technology company deploying code several times a day cannot rely on an IT audit conducted over three weeks each year. The coverage gap is stark: conventional audit methodology typically examines somewhere between three and five percent of an organisation's total transaction population. The remaining ninety-six percent remains untested.

Add to this the explosion of unstructured data — emails, contracts, regulatory filings, third-party correspondence — and the picture becomes clear. The traditional internal auditor, however skilled, was always fighting a losing battle against data volume.

What AI Actually Changes

The entry of artificial intelligence into the audit arena is regularly defined within the breathless language of disruption. The facts are more nuanced and in many cases more exciting.AI does not replace professional

judgment. What it does do is significantly expand the surface approximation over which that judgment can be implemented. Process mining technology can reconstruct the actual flow of industrial business practices from device logs, revealing deviations from alleged controls without a human interaction. The time-allocation shift this enables is profound. Where auditors once spent the majority of their working time on data gathering, extraction, and basic testing — essentially manual labour — AI-augmented teams can redirect that capacity toward interpretation, risk judgment, and stakeholder dialogue.

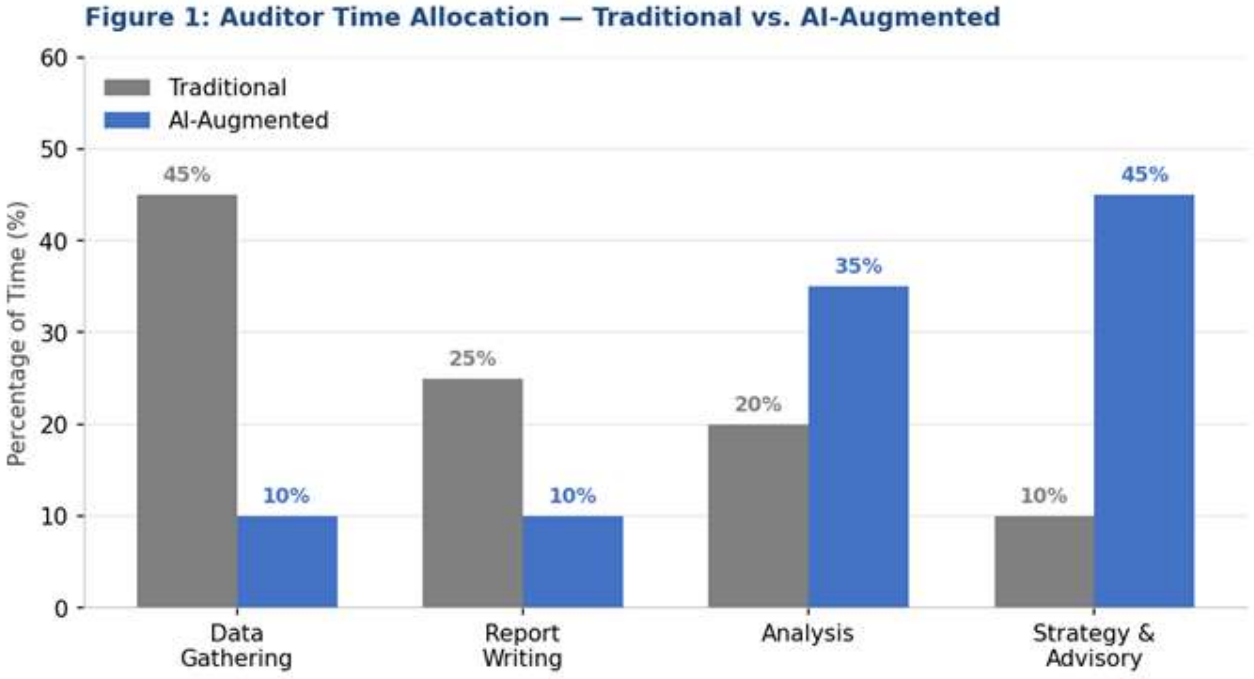


Figure 1: Auditor Time Distribution — Traditional vs. AI-Augmented function. Source: IIA Book 2023; Deloitte Internal Audit Survey 2023.

Continuous Monitoring: From Annual Cycle to Incessant Vigilance

Perhaps the most consequential shift enabled by AI is the transition from periodic to constant auditing. Traditional audit plans operated on an annual cadence because annual cadences were what humans could manage. AI removes that constraint entirely.

Continuous monitoring frameworks — already deployed by leading audit functions at global banks, pharmaceutical companies, and government agencies — use rule-based and machine-learning models to run automated tests across defined control populations every day, sometimes every hour. When a payment exceeds threshold, when a journal entry is posted outside business hours, when a procurement transaction bypasses the three-way match, the system flags it immediately. Audit teams receive curated exception reports rather than raw data dumps, allowing them to investigate .

Many excessively high-profile corporate frauds in recent decades lasted precisely because they fell between the cracks of regular audit cycles. Continuous monitoring significantly reduces those cracks. The coverage, which when carried out to about four percent of transactions can, in order, be amplified to one hundred percent — not via human evaluation of each object, however via automated screening that escalates real exceptions to human attention.

Figure 2: Transaction Coverage — Traditional Audit vs. AI-Enabled Monitoring

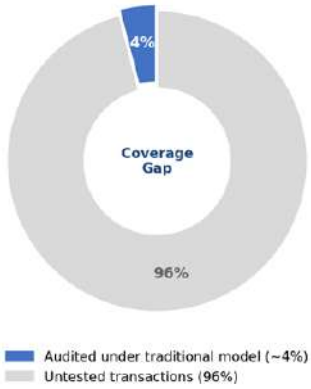


Figure 2: Transaction coverage gap — Traditional pattern-based total audit (~4%) vs. AI-enabled non-stop monitoring (up to 100%). Source: PwC The State of the Internal Audit Profession 2024.

The Predictive Frontier: From Certainty to Anticipation

Beyond continuous monitoring lies a further frontier: predictive audit intelligence. This is where AI begins to alter not just how audits are conducted, but what questions they ask.

Predictive analytics tools can identify which business units, processes, or control environments are most likely to produce significant findings — before a formal audit engagement begins. By training models on historical audit results, financial performance indicators, headcount changes, and operational metrics, these systems can produce risk scores that guide audit planning with a precision no subjective risk assessment can match.

Some organisations are going further, deploying AI to model systemic risk scenarios — effectively stress-testing their own control environments against hypothetical conditions before those conditions materialise. In regulated industries, this capability is beginning to attract genuine interest from boards and audit committees who want audit functions that can anticipate regulatory scrutiny rather than respond to it.

The Skills Imperative: Auditing the Auditors

Transformation at this scale creates an uncomfortable question for audit leadership: does the current workforce have the skills to deliver it? The answer, candidly, is that most audit teams do not — yet. The Institute of Internal Auditors' Global CBOK studies have consistently found that data analytics capabilities lag expectations across the profession. Many audit functions have data analysts embedded within them, but relatively few have achieved the integration required to make analytics a routine part of every engagement rather than a specialist add-on.

Closing this gap requires investment in three directions simultaneously. First, technical upskilling: auditors at every level need adequate record-keeping capability to interrogate AI outputs, challenge. Second, tool adoption: the market for audit-specific analysis systems has matured significantly, and functions that now do not but have adopted committed tooling are an increasing number of behind the curve. Third—most important—cultural choice: the internal auditor's identification has traditionally been based on procedural knowledge and date capital. Embracing AI requires a willingness to give up burdens of the manual craft that defined careers while investing in new skills that we feel are unconventional.

Figure 3: Internal Audit Capability Maturity by Domain (Score out of 5)

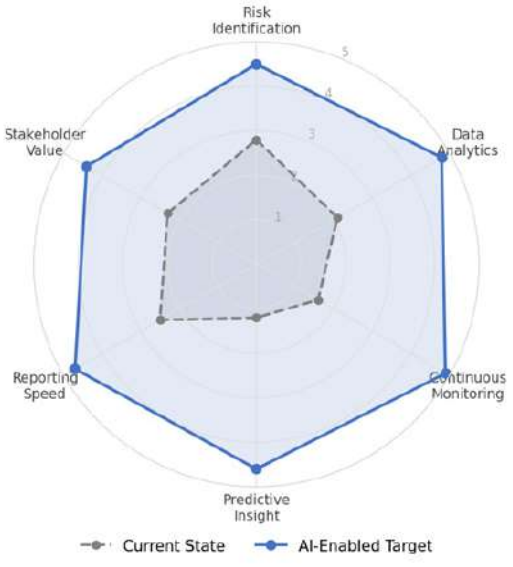


Figure 3: Internal audit capability maturity via region (rating out of 5) — Current nation vs. AI-enabled frontier. Sources: IIA Book 2023; Protiviti Internal Audit Survey 2023; KPMG Internal Audit Outlook 2024.

Governance, Autonomy, and the Limits of Automation

The erosion of professional independence through algorithmic dependency.

When an AI model surfaces a finding, the human auditor's role is to evaluate it — not to ratify it. This distinction matters more than it might appear. Machine learning models are trained on historical data and encode the assumptions embedded in that data. They are excellent at detecting patterns that resemble past anomalies and poor at identifying genuinely novel risks —An audit function that becomes too deferential to its own AI tooling may develop a false sense of coverage while becoming progressively less capable of the imaginative, sceptical thinking that produces the most important audit findings.

There are also meaningful questions about explainability. When an AI flags a transaction as anomalous, the auditing standard of care requires the auditor to understand why. Black-box models that produce results without interpretable reasoning create a professional and regulatory exposure that audit leadership must actively manage. The most forward-thinking functions are building explainability requirements directly into their tool selection criteria.

Data governance presents a related challenge. AI-driven audit functions ingest large volumes of sensitive business data. Ensuring that data is handled in accordance with privacy obligations, protected against misuse.

The Audit Function of 2030

The internal audit function that emerges from this transformation period will look meaningfully different from the one that entered it. Its testing will be continuous rather than periodic. Its risk identification will be data-driven rather than interview-dependent.

More fundamentally, it will have reclaimed the strategic positioning that the profession has always aspired to but rarely achieved. When audit leaders are freed from the administrative burden of data collection and basic testing, they become genuine risk intelligence partners to the board — offering foresight, not just hindsight.

The organisations that will benefit most are those that treat AI adoption in internal audit not as a cost-reduction exercise but as a capability investment. The goal is not fewer auditors doing the same work more cheaply. It is the same auditors — or, with growth, more of them — doing fundamentally more valuable work.

The third line of defence is being redrawn. The question for every audit leader is not whether AI will reshape their function, but whether they will shape that transformation or be shaped by it.

INTERN L UDIT REIM GINED

Redefining the ssurance Function in the ge of rtificial Intelligence

Nitish Jha , Nitin Kumar
Scholar Batch 17,Global Risk Management Institute (GRMI)

Abstract

The internal audit profession is at a turning point. Artificial Intelligence is now changing how assurance and control evaluation work. It used to be limited to tech companies and research labs. Now AI is redefining audit in a big way. This includes changing what internal audit does how it does it and what value it provides. Internal audit is moving from checking things every then to always keeping an eye on things using data. The authors of this article looked at whats happening in the industry and new guidelines. They think auditors who use AI as a helper will be able to do their job faster. This will also help auditors give useful advice to their organisations. The internal audit function will become more important to their organisations. Auditors who work with AI will be able to find issues and fix them quickly.

Organisations will benefit from having control and assurance. Internal audit will be able to provide strategic advice using AI. The future of audit is, about working with AI.

Introduction: The Tectonic Shift

For decades, internal audit followed a familiar routine, completing annual risk assessments, quarterly audit plans, and periodic sampling of transactions. The profession's value came from a clear methodology, professional skepticism, and human judgment. This foundation is still important. However, the environment in which it operates is changing quickly and on a large scale, requiring a complete rethink of how audit work is done, governed, and communicated.

AI (which encompasses machine learning, natural language processing, robotic process automation, and generative AI) is not something for which we need to worry about in the future. AI is now. In fact, more than 61% of CAEs admitted to having AI risks in their top five categories of organizational risks per the IIA 2024 Pulse of Internal Audit survey, but

fewer than 30% admitted to significantly integrating AI into audit processes (IIA, 2024). This divergence in organizational risk vs. Audit process tools can be the key challenge and a critical opportunity.

This article looks at how AI is changing internal audit—not by replacing human auditors but by significantly enhancing what they can see, analyze, and ensure.

From Sampling to 100% Population Testing

One of the biggest changes AI brings to internal audit is the ability to move from statistical sampling to full-population testing. Traditional audit methods are shaped by resource limits and time pressures. They usually look at 5 to 10% of a transaction population and rely on statistical inference to make conclusions about the entire group. This method, while acceptable, carries risks. Anomalies and irregularities in the untested 90 to 95% can go unnoticed.

AI-powered data analytics tools, such as ACL (now Galvanize), IDEA, and custom-built machine learning systems, allow auditors to access and analyze entire datasets. Every journal entry, every vendor payment, and every access log can be evaluated against defined risk criteria at the same time. Outliers, duplicates, unusual patterns, and control exceptions are identified automatically. This helps auditors focus their attention on areas with the highest risk.

Real-World Example

A top financial services firm used a machine learning-based continuous monitoring system in its accounts payable function. In the first quarter, the system flagged 847 transactions for human review. It uncovered three cases of vendor fraud that had avoided traditional controls. The total recoverable losses were Rs. 4.2 crore. The time to detection was 72 hours compared to a median of 14 months in previous years.

This has a significant consequence on audit planning. Assessment of risks will not be a year long annual affair but a real time, on going activity. The actual audit resources could then be deployed in real time as risk signals arise, rather than static, pre- planned audits.

AI Augmentation: The Auditor as Analyst and Strategist

The popular concern that AI will make auditors irrelevant will not come to fruition. The exact opposite appears to be the case, with AI replacing high-risk, mundane work and instead allowing auditors to focus on the higher value, consultative aspects of auditing that machines are incapable of.
Let's think about the audit lifecycle. In the past, the audit cycle was made up of 60-70% of time spent collecting, reconciling and documenting data. Automated systems – from RPA bots gathering data in its preferred format and NPL engines extracting information from contracts, policies and procedures – will make this phase very small, with the majority of an auditors time spent on analytical assessment and interpretation, working with stakeholders and giving strategic advice.

Comparative Impact: Traditional vs. AI-Augmented Internal Audit

Area	Traditional IA	AI-Augmented IA
Risk Assessment	Annual / periodic	Continuous, real-time
Sample Size	5–10% of population	100% of transactions
Anomaly Detection	Manual review	Automated ML flags
Report Turnaround	Weeks	Hours to days
Fraud Identification	Post-event	Predictive / preventive
Auditor Focus	Data gathering	Analysis & judgment

This paradigm shift profoundly alters the internal auditor's competency profile. Data literacy, analytical thinking, and translating algorithms into business insight are skills as-arguably more-important as documentation skills of internal auditors. The new Global Internal Audit Standards (2024) from the IIA explicitly include technological competence as a competency, indicating a sector-wide awareness of this development.

Auditing AI: The Emerging Frontier

Now that AI is increasingly used in organisational decision-making-in areas such as credit scoring, procurement selection, customer segmentation and regulatory reporting-internal audit is being given a new, intimidating job: auditing AI itself. This area is likely to be new and alien to many functions, requiring skills well outside those for financial and operational audit. Risk areas in audit of AI include: model risk (whether the model is accurate, relevant and fit-for-purpose); data integrity risk (whether training data is representative, free from bias and well governed); explainability risk (whether decisions can be justified and questioned with auditors and regulator); and ethical risk (whether the model reflects and exacerbates bias towards protected groups).Establish a dedicated AI/Model Risk audit programme within the annual plan.

Create or purchase adequate tools for model validation, testing for bias and establishing interpretability of the model.

Utilize experts – data scientists, AI Ethicists – as co-sourcing partners to an audit team.

Integrate audit procedures with the forthcoming guidelines, particularly ISO/IEC 42001 (AI Management Systems) and SEBI/RBI AI governance rules applicable for India.

This issue is especially sensitive for Indian organizations, given the rapid uptake of AI in financial services (BFSI), healthcare and the public sector. The recent 2024 guidelines of the Reserve Bank of India for management of model risk within regulated entities make it implicitly clear that audit of AI needs to be part of governance based controls, not an option.

Governance, Ethics, and the Human Anchor

No review of AI in internal audit would be complete without acknowledging its risks. Systems have been shown to build in biases, produce believable (but wrong) output (hallucination is typical in generative AI) and produce audit trails that are difficult to explain and defend. The paradox of automation where over-reliance on automated toolsets lead to complacency and a lack of professional skepticism. Any governance framework for an AI-enabled audit would need to stand on three legs. The first is human supervision: AI outputs need to be vetted and checked by a competent auditor prior to it leading to a finding or the production of a report. Second, explanation: the team need to be able to understand how the AI tool arrived at its conclusion, internally and to auditees. Third, recalibration: the tool must be re-tested for validity, bias and relevance at regular intervals, and to take into account changes in the organizational risk profile and underlying data set.

The Ethical Imperative

As AI raises more alerts, the role of the human auditor will not diminish, but become more crucial. Algos have no moral capacity; the auditor-prompted by the IIA Code of Ethics, professional judgment, and organizational knowledge-determines whether the alert indicates a breakdown of control, a statistical anomaly, or a real business anomaly. The algorithm escalates, the auditor decides.

Recommendations: Building the Audit Function of Tomorrow

To audit students and young auditors, the message is stark and immediate: invest in the non-replicable skills that AI can't match and the level of technical competence to work alongside AI tools comfortably and productively.

Data Analytics: Acquiring skill in tools like Python, SQL, Power BI, and specific audit tools like ACL or IDEA is now almost a table stakes requirement.

AI Literacy: Developing a fundamental understanding of how machine learning models work-including their assumptions, limitations, and how they fail-will be crucial for auditing AI and utilizing it in a safe and effective manner.

Reinforce Professional Skepticism and Critical Thinking: Asking the "right" question that an algorithm cannot pose remains the ultimate differentiator for the auditor of the future in the AI-enabled world.

Engage with New Standards: The recently revised Global Internal Audit Standards (2024) from the IIA and ISACA's frameworks are provide solid, profession-specific advice on AI.

Champion the Establishment of ethical AI governance at your organizations: Internal audit is perfectly situated to offer independent assurance over the fairness, transparency, and the degree of deviation within stated risk tolerance of AI systems.

Conclusion

The internal audit profession is not being replaced by AI, it is being reinvented by it. The internal audit function that sat at the periphery of the organisation's strategy-making is now being empowered, with both the technology and the data access, and the mandate, to sit at the heart of organisational governance. The auditors of this new generation of the function will be those who can combine both technical competence with utmost integrity, who view AI not as a threat but as a tool that provides internal audit with the greatest opportunity in the history of the profession to do what it exists to do – provide independent, objective assurance and advice in which organisations can place their trust to protect and create value.

The choice facing every internal auditor in practice is no longer whether or not to adopt AI – the sheer speed of organizational transformation has made this an exigent reality. The choice now facing us all is the extent to which we will adopt AI appropriately, ethically, and with the same level of technical proficiency as this assurance function requires.

The I Imperative in Internal udit

From Compliance to Strategic dvisory

Tanisha Dua, Yashas V, Ashwini Chauhan
Scholar – Global Risk Management Institute (GRMI)

Introduction

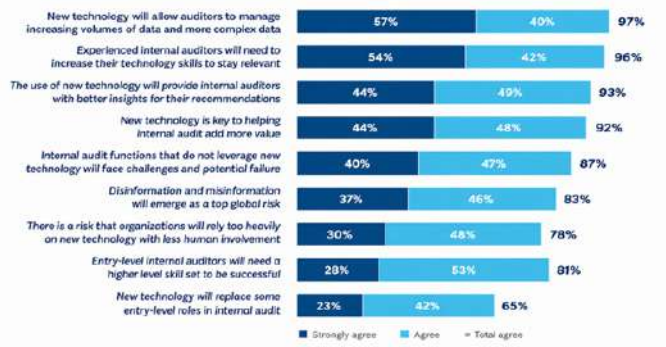
Artificial Intelligence (AI) is no longer a futuristic concept; it is the new frontier of corporate governance. As organizations grapple with complex digital ecosystems, internal audit functions face mounting pressure to deliver faster insights, deeper data analytics, and real-time assurance all without expanding their budgets.

To survive this shift, audit professionals must evolve from traditional, compliance-focused checkers to proactive, strategic advisors. Generative AI (GenAI) is reshaping traditional workflows by introducing efficiency and depth at every stage of the audit process, from automating documentation to analyzing large datasets.

Recent research, including studies by Eulerich et al. (2025), confirms that integrating AI into internal audit significantly improves overall audit quality, risk assessment accuracy, and operational effectiveness. However, failure to adopt AI may result in other functions taking the lead in governance and risk oversight.

To remain relevant, audit functions must integrate AI into their strategy, processes, and skillsets while ensuring human judgment, oversight, and independence are maintained.

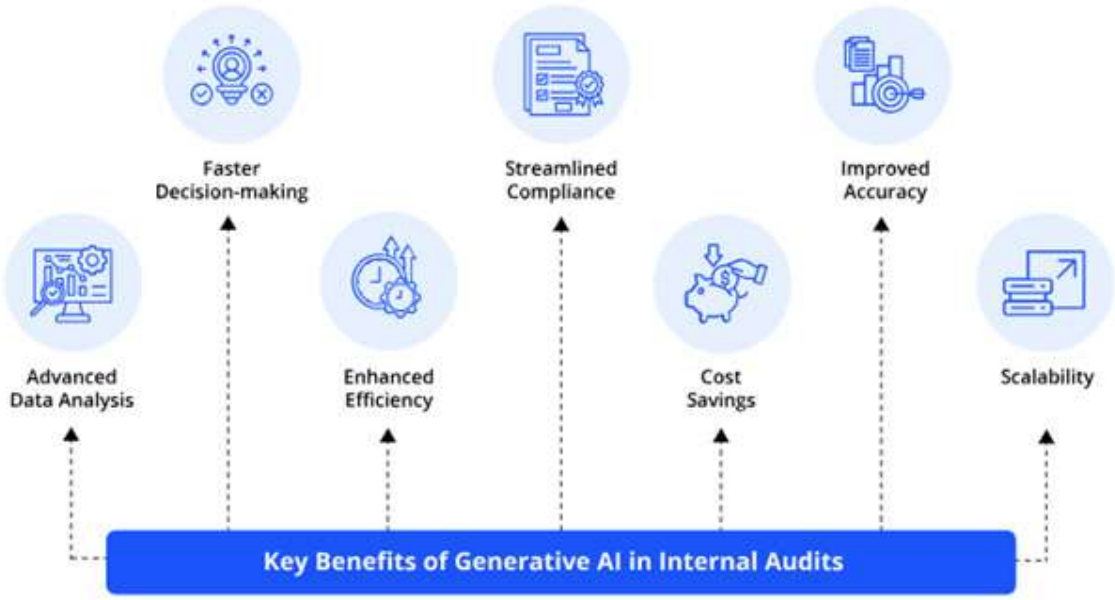
Technology Adoption and Skills Consensus in Internal Audit



Traditional vs AI-Enabled Internal Audit (with Examples & Stats)

Audit Dimension	Traditional Internal Audit	AI-Enabled Internal Audit (Examples & Stats)
Efficiency	Manual, labor-intensive	RPA reduces manual work by 30–50% (e.g., automated reconciliations in finance audits)
Risk Identification	Periodic, delayed detection	Continuous monitoring → risks flagged instantly (e.g., real-time vendor risk dashboards in TPRM systems)
Fraud Detection	Rule-based, reactive	AI detects anomalies in real time (e.g., HSBC uses ML for AML fraud detection) → fraud detection rates improve by 2–3x
Third-Party Risk (TPRM)	Annual vendor reviews	Dynamic risk scoring + continuous monitoring (e.g., AI scans sanctions lists, news, ESG risks in real time)
Cybersecurity Auditing	Reactive incident response	AI-driven threat detection (e.g., SOC automation) → reduces breach response time by up to 70%
Cost Structure	High recurring labor costs	Cost savings 20–40% via automation (PwC estimates)
Audit Role	Compliance-focused	Strategic advisor (e.g., AI-driven ESG risk insights, predictive risk modeling)

Key Benefits of Generative AI in Internal Audits



Intelligent Automation and Advanced AI in Risk Management

- **Transforming Third-Party Risk Management (TPRM)**

AI and intelligent automation are transforming how organizations manage risks from vendors and third parties. Instead of relying on periodic, manual reviews, companies now use continuous, data-driven monitoring to identify and respond to risks in real time. This improves efficiency, accuracy, and proactive risk mitigation across the entire vendor lifecycle.

Key Points:

- AI classifies vendors into risk levels (dynamic risk tiering)
- Automates vendor assessments and questionnaires
- Continuously monitors external data (news, sanctions, risks)

Example:

A bank's AI system flags a vendor due to negative regulatory news, updates its risk rating instantly, and alerts the team to review or replace the vendor.

- **Cybersecurity and Intelligent Incident Response**

AI-driven cybersecurity refers to the use of artificial intelligence to monitor, detect, and respond to cyber threats in real time. It shifts security operations from manual, reactive approaches to automated, proactive defense systems that can act instantly.

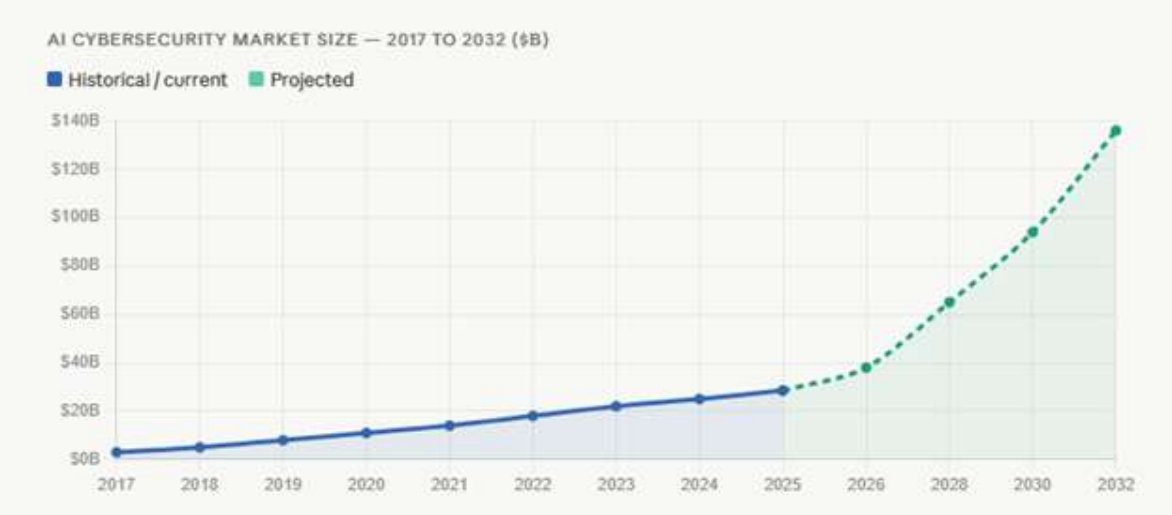
Key Points:

- AI continuously monitors networks, cloud systems, and endpoints
- Detects threats in real time using advanced analytics
- Automates responses (e.g., isolating devices, triggering playbooks)
- Reduces incident response time significantly

Example:

An AI security system detects unusual activity on a company server, automatically isolates the affected system, and initiates a response protocol—preventing a potential breach within minutes.

AI Cybersecurity Market Growth Respresentation



Advanced Data Loss Prevention (DLP)

AI-driven DLP uses behavioral analytics and NLP to protect sensitive data by monitoring user activity and detecting anomalies in real time.

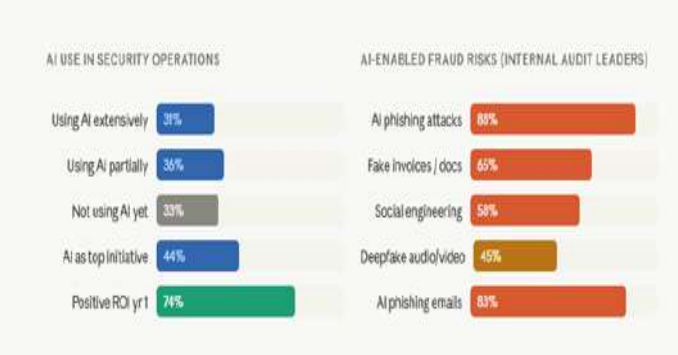
Key Points:

- Establishes normal user behavior patterns
- Detects anomalies (insider threats, data leaks)
- Uses NLP to scan emails and documents

Example:

An AI system detects an employee downloading large confidential files at unusual hours and blocks the transfer automatically.

AI in Security & Emerging Fraud Risks Representation



Automating Governance & ESG Strategies

AI and automation support ESG goals by improving data tracking, compliance, and decision-making across environmental, social, and governance areas.

Key Points:

- Tracks sustainability data (energy, emissions)
- Uses AI to reduce bias in hiring
- Ensures ethical supply chains via blockchain
- Automates compliance and reporting (RegTech, RPA)

Example:

A company uses AI and IoT sensors to monitor carbon emissions in real time and generate automated ESG reports.

AI Adoption, Market Growth, and Risk Metrics: A 2025–2030 Snapshot

Case Studies and Practical Applications

- **Goldman Sachs leverages AI/ML in Third-Party Risk Management (TPRM)** to enhance vendor oversight across a large supplier base.

Key Applications

- ML-driven risk scoring processes 500K+ data points daily, covering cybersecurity, financial health, and geopolitical risks
- NLP tools analyze 100% of 2,500+ annual contracts, automatically flagging 85% of compliance risks
- Model Risk Management (MRM) oversees 200+ AI models, reducing false positives by 40% while ensuring human oversight

Deutsche Bank: AI & ML in TPRM (2026 rollout)

Deutsche Bank expands AI/ML capabilities in Third-Party Risk Management (TPRM) across 18,000+ vendors, enhancing efficiency, accuracy, and proactive risk detection.

Key Applications

- AI automates 97% of vendor onboarding, reducing time from 60 days to 22 days with 99.5% accuracy
- Machine learning validates 1.8M documents annually across 700+ data sources
- Behavioral analytics identifies 90% of anomalies across vendor systems in real time
- NLP analyzes contracts and flags up to 93% SLA violations and 89% compliance issues instantly

- AI-driven supply chain mapping uncovers hidden risks in 33% of cases, improving risk visibility by 44%.

Key Implementation Challenges and Risks

Adopting emerging technologies introduces serious challenges that internal audit functions must assess and manage:

- Hallucination & Accuracy Risk: GenAI can generate incorrect or completely fabricated results. Relying blindly on unverified AI models can materially damage audit quality and credibility.

- Data Privacy & Confidentiality: Uploading sensitive organizational data into public AI models can violate data protection regulations (e.g., EU GDPR or India's DPDP Act).

- "Black Box" Problem (Lack of Model Explainability): Complex deep learning outputs are often opaque, making it difficult to demonstrate defensible and transparent audit conclusions to regulators.

- Over-Automation Risk: The risk that auditors become overly reliant on automated systems, leading to a loss of professional skepticism. The human-in-the-loop component cannot be eliminated.

Strategic Implementation Best Practices

- Prioritize Strategic Risks: Focus on threats that can significantly impact the organization's success rather than just operational risks.
- Establish Dedicated AI Governance: Develop purpose-built AI usage policies and controls, ensuring that audit tools are secure and independent.
- Elevate the Skillset: Expand the internal audit team's capabilities to encompass data analytics, scenario planning, and expertise in emerging threats like cybersecurity and ESG.

Questions

- How is AI reshaping internal audit from compliance to a strategic role?
- How does AI improve audit effectiveness compared to traditional sampling methods?
- How can AI be governed in internal audit while ensuring compliance and ethics?
- What is the role of human judgment in AI-driven internal audit?
- How is AI used in fraud detection and risk identification in internal audits?

Conclusion

In conclusion, internal audit has a significant opportunity to enhance its strategic value by leveraging advanced technologies such as artificial intelligence, machine learning, and blockchain. These tools enable a shift from reactive, retrospective assessments to proactive, data-driven insights, supporting real-time risk identification and more informed decision-making across areas like third-party risk management, cybersecurity, data protection, and fraud detection.

At the same time, this transformation must be approached thoughtfully. Challenges related to data quality, governance, skill gaps, and ethical use of AI require careful and strategic management. By addressing these considerations and balancing technological innovation with professional judgment, internal audit can strengthen its role as a trusted, forward-looking advisor and continue to add meaningful value to the organization.

The ugmented udit

Fuelling I Insight

Prajakta Buggewar & Satyanarayan Patro
Scholar – Global Risk Management Institute (GRMI)

Abstract

Technology is rapidly changing the way internal audit works – moving away from being a periodic compliance function, to one that provides strategic assurance. The explosion of digital business models and the adoption of advanced technologies, coupled with increasing speed and complexity in organizations leads to very dynamic organizational risks. While technology has allowed the internal audit function to leverage data and automate many of the traditional audit processes, internal audit must also adapt to new and innovative ways of providing assurance. The future of internal audit will depend on cooperation and the integration of AI based analytical tools with auditors' timely professional judgment so they can identify the emergence of risks earlier, assess control effectiveness more frequently and assist with governance issues before they become threats to the organization.

Introduction

With a transaction approvals and decisions travelling at speed that traditional audit cycles were never designed to keep pace with, modern organizations operate in an environment of continuous activity. As a result, automated workflows, digital platforms, and AI-based systems have enhanced operational efficiency while also increasing the complexity of risks associated with these operations. Consequently, internal audit can no longer be restricted to the past compliance check. It needs to be far more agile, strategic and integrated into enterprise governance.
This shift is especially important because AI is altering the way we make business decisions, and how controls work in practice. Internal audit must therefore broaden its embrace to inspect not just traditional process areas but also data quality, model governance, algorithm accountability, and the degree of human oversight. In this sense, rather

than abandoning its person-centric identity, the audit profession is then reframed as an element that merely broadens the strategic relevance of a firm.

The Growing Importance of Internal Audit

The role of internal audit has been predominantly focused on obtaining assurance over internal controls, compliance and operational effectiveness. Such tasks remain critical but are no longer adequate in a digital environment: threats can appear from one to another system and develop at an alarming rate. Stakeholders are expecting internal audit to provide deeper insights into new emerging threats, underlying structural control weaknesses and the wider impact of technological change today.

And this wider alignment commands a change of mind-set. Internal auditors will have to shift from reviewing sample exceptions to being able to see the drivers of risk, systemic vulnerabilities and organization blind spots. The profession is being called on more and more to furnish early-warning intelligence as opposed to post-event assurance. This means that internal audit becomes a more involved partner in resilience, accountability and strategic decision-making.

Science and skills in AI Era

Balancing science and skill is the key to the future of internal audit. The scientific aspect involves data analytics, continuous monitoring, exception testing, and using artificial intelligence (AI) to evaluate large populations of transactions in ways that traditional sampling methods alone cannot. AI can help to identify unusual patterns, compare operational actions over time, and highlight likely gaps in controls based on information collected in close to real-time.

Although AI can help identify anomalies; it cannot, by itself, determine if those anomalies represent either a legitimate business complexity, weak internal controls or a significant failure in governance. The application of professional scepticism, the interpretation of information in context, and maintaining independence are essential for producing high-quality audit work. The effectiveness of internal audit will therefore be enhanced in the AI era not by replacing human judgement, but rather by augmenting human judgement through the use of better tools and enhanced visibility across multiple sources.

Use of Timeliness as a Method of Control

The establishing criteria for effective internal audit is determined through timeliness. With digital environments in place, risk can propagate through systems, vendors, and controls at an ever-increasing rate. As a result, detecting problems later than sooner will cost organizations additional money and create challenges. The sooner a problem is identified, the more likely it is for managers to remedy deficiencies, maintain adequate documents for recordkeeping purposes, and mitigate potential damages to the business (operationally, or otherwise).

As such, the internal audit department must not be confined to just fixed audit periods. There are additional responsibilities to be fulfilled, which include on-going computer surveillance of operations, more rapid escalation of issues, and reporting audit findings in a manner that enables a more responsive manner with respect to their findings. While providing timeliness is primarily an efficiency matter; it is also a critical to the governance principle associated with determining whether or not audit insights are available for action at the time they can be acted upon.

AI Can Be a Force Multiplier for Audit

Although AI is not intended to replace auditors,

audit professionals should see it as a force multiplier for their audit capabilities including the ability to increase the volume of transactions reviewed; speeding up the detection of anomalies and more responsive monitoring of risks across multiple functions such as finance, operations, technology and regulatory compliance; enable internal audit to have greater scale and speed of work as well as produce more precision with their findings.

At the same time, internal audit needs to evaluate and understand he knew risks associated with AI, including poor quality data, lack of transparency in model behaviour, weak governance over automated decisions and over-reliance on tools that may seem objective but are not adequately validated. Therefore, internal audit has two responsibilities related to AI:

(1) To utilize AI carefully in its own methodology
(2) To evaluate the organization's governance related to the use of AI.

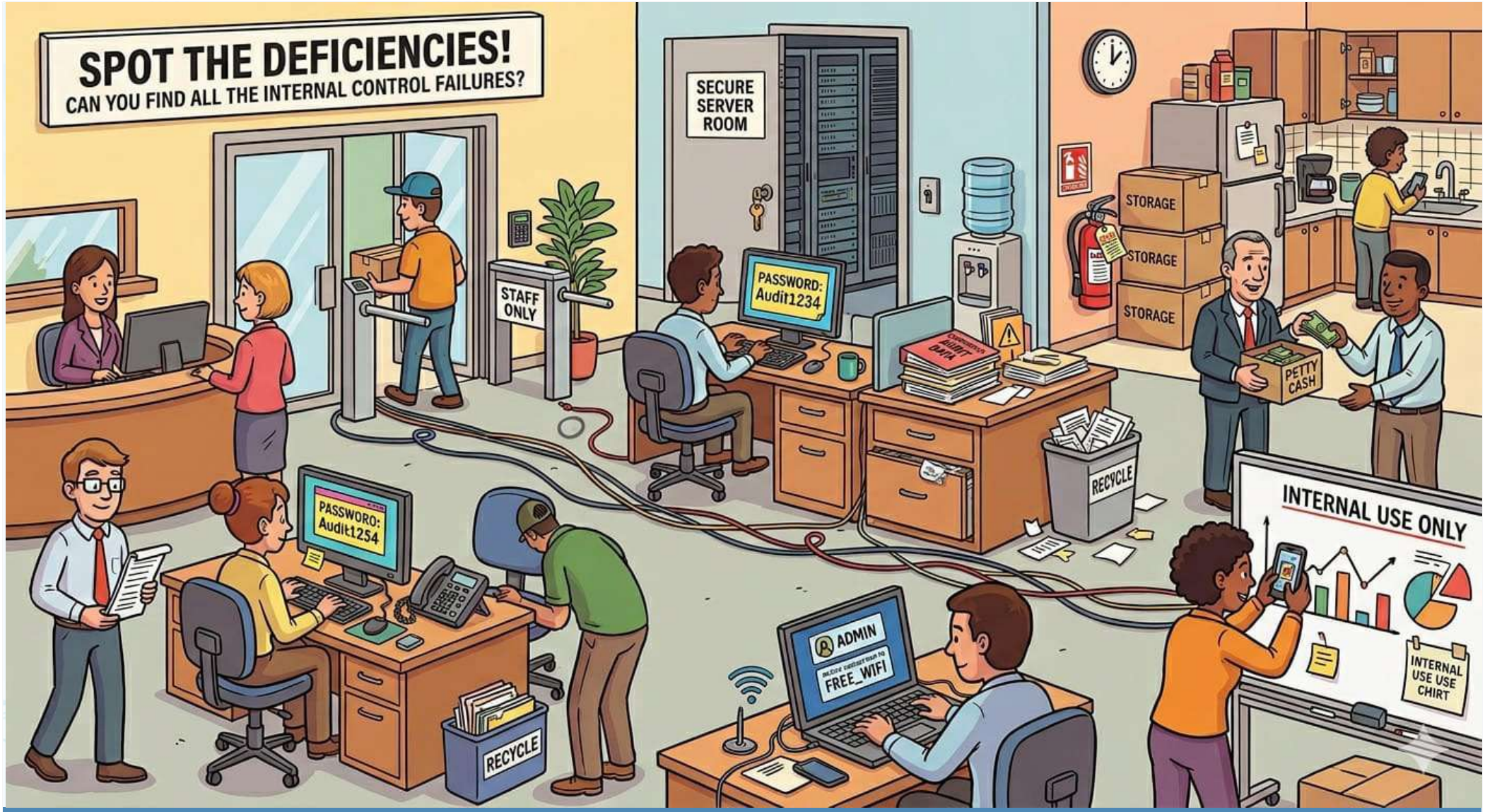
Governance and strategic relevance

With the rise of AI, boards and senior executives are placing greater reliance on internal audit. As AI is introduced, monitored, controlled, and aligned with an organization's risk appetite, senior leadership and governance bodies are looking for assurance. Because internal audit can assess both the technical and control aspects of AI adoption, it is uniquely positioned to provide this assurance.

To do this, internal audit must be independent, have direct access to relevant data, and invest in new capabilities, including analytics, AI governance literacy and technology risk assessments. Organizations that modernize their internal audit function will have a higher rate of determining emerging risks early, better accountability and more trust in an increasingly automated world.

Summary

The function of internal audit is going through a period of redefinition. This transformation will take place as a result of three factors: The confluence of artificial intelligence, the complexities of digital technology and increased expectations for strategic assurance. The future of internal auditing will involve the integration of technological capability with human judgment to ensure that the internal audit function will continue to be timely, relevant and effective in an environment that presents ever-changing risks. In this age of artificial intelligence, the role of the internal auditor is no longer limited to serving as a checkpoint to verify that processes are being followed but also as a contributor to strong governance and sound decision making.

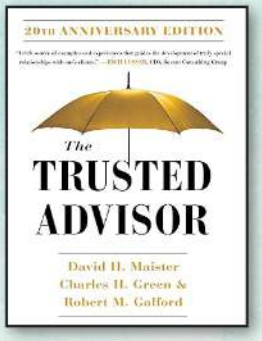


Sharpen Your Mind: The I Quiz

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

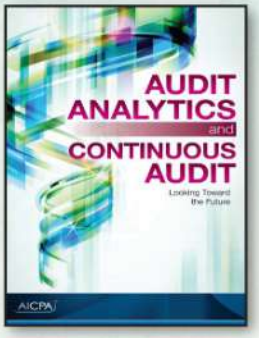
BOOKS THAT MATTER

Top Picks for IA Professionals



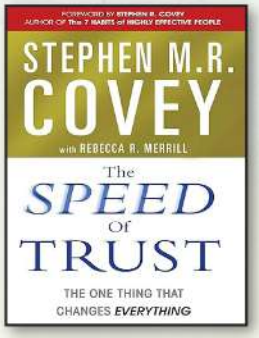
Trusted Advisors

A powerful read for internal auditors aspiring to become strategic partners to business leadership. The book highlights how internal auditors can build influence, trust, and long-term organizational value by moving beyond traditional assurance roles and embracing advisory thinking.



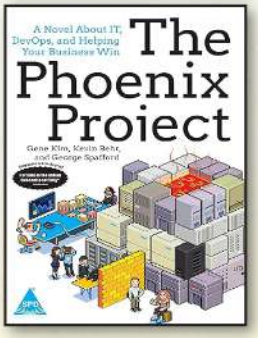
Audit Analytics and Continuous Audit

This book offers practical insights into the growing role of data analytics, automation, and continuous auditing within modern internal audit functions. It serves as a valuable guide for auditors seeking to strengthen technology-enabled assurance capabilities.



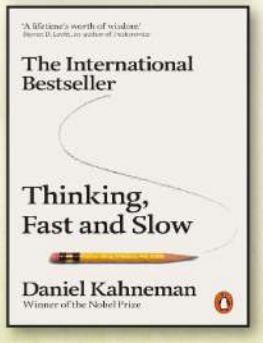
The Speed of Trust

An insightful book that explores how trust influences leadership, governance, culture, and organizational performance. For internal auditors, it reinforces the importance of integrity, credibility, and transparent communication in building stakeholder confidence.



The Phoenix Project

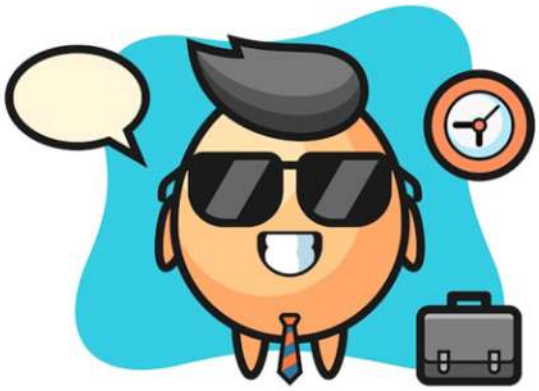
Written in a storytelling format, this book provides deep understanding of IT operations, process management, cybersecurity challenges, and digital transformation. It helps internal auditors better appreciate operational dependencies and technology risks in today's organizations.



Thinking, Fast and Slow

A globally acclaimed book on decision-making and behavioral psychology that explains how biases influence judgment and risk assessment. It encourages auditors to strengthen analytical thinking, professional skepticism, and objective evaluation during audits.

Humour in Action



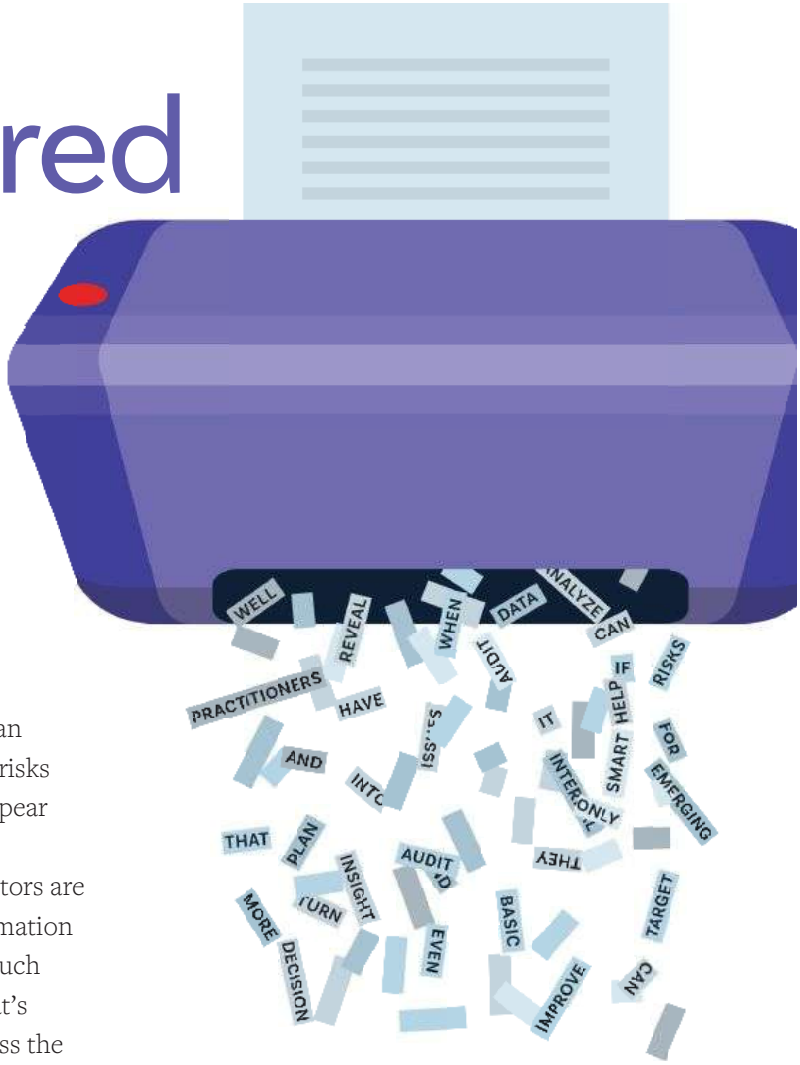
AROUND THE WORLD AUDIT INTELLIGENCE FROM ACROSS THE WORLD

tech

Unstructured Insight

Auditors can turn data from disparate documents into clear signals that focus their reviews.

Shwathama Rajendran



Structured data is easy: It's clean, organized, and ready for analysis. But studies by firms such as Gartner and IDG estimate that about 80% to 90% of data is unstructured — think Word documents, PDFs, emails, and many other formats.

These documents don't follow any analytical rules, so internal auditors often overlook them because they may not have the tools or the time to analyze large volumes of unstructured data. Yet, the documents contain some of the internal audit function's most valuable insights. For example:

- Issue documents, such as audit findings, incident reports, and compliance reports, can reveal recurring control problems across business areas.
- Audit reports often contain clues about common root causes.
- Risk assessments can highlight emerging risks long before they appear on dashboards.

When internal auditors are able to pull this information together, they get a much clearer picture of what's really happening across the organization. That can lead to better planning, stronger conversations with stakeholders, and smarter decisions. Several practical methods can help internal audit unlock these insights from unstructured data.

Natural Language Processing

Suppose internal audit needs to pull themes from several Word documents stored on a Google Drive or a local drive. The Python programming language makes it easy to scan files from several folders and read the contents. Auditors can use Python Operating System libraries to parse the files.

Next, auditors need to convert the text data into a single unit of meaningful text, called a token, by breaking it into individual words. They also must remove words called stop words, such as "and," "is," and "the," that add little value to analyses. Auditors can use Python to remove stop words, and they can customize the stop word list.

From there, auditors could simplify the token by removing inflectional word endings, returning words to their base form (for example, changing "eating" to "eat"). This process, called lemmatization, makes the data ready for different types of analysis.

N-gram analysis. This type of analysis identifies common themes by counting how often word pairs or triplets — for example, "regulatory compliance" or "regulatory compliance framework" — appear across documents. Using Python libraries like NLTK or spaCy, internal auditors can quickly generate n-gram frequency tables and store them in a data frame along with metadata such as author, date, or business area. This makes it easy to filter themes by region or process.

For example, while they are reviewing emails and Word documents about data security compliance, auditors might notice that word pairs such as "data breach" and "security vulnerability" come up often. This might indicate recurring security issues.

Auditors can use visual tools or word clouds to highlight the most frequent phrases. This is a simple but powerful way to uncover recurring concepts in audit reports or issue documents.

Named Entity Recognition (NER). Internal auditors can use NER to extract key details such as locations, business units, vendors, and product names from large volumes of text, eliminating the need to manually scan issue documents or reports. This information can reveal important risk patterns.

For example, recurring locations may indicate higher residual risk, and repeatedly mentioned vendors or processes may signal systemic control gaps. By finding these trends quickly, NER helps auditors refine their scope to focus attention where it is most needed.

Latent Dirichlet llocation (LD). This method of topic-modeling groups documents into themes based on words that frequently appear together. It can help internal auditors uncover patterns they may not think to look for. For example, running LDA on several years of audit reports might quickly reveal risk themes that are trending, such as:

- Problems with access management, password resets, and privileged accounts.
- Questions about encryption and data transfer.
- Gaps in vendor oversight, service-level agreements, and third-party monitoring.

Internal auditors can use Python's Gensim library to generate themes and identify which topics each document relates to, while libraries like pyLDAvis make them easy to visualize.

Sentiment nalysis. By using a few lines of Python code, auditors can determine whether the sentiment of a document is positive or negative. Auditors who run this analysis when they are writing reports for stakeholders can identify and change words that are too negative.

For example, sentiment analysis might show that a report on a vendor's performance has a negative tone because it contains phrases like "unsatisfactory service" or "failed to meet expectations." Auditors might change the report to use a more neutral term such as "service needs improvement."

Machine Learning

Depending on the use case, internal auditors can apply machine learning methods to unstructured data. For example, classifying algorithms can help auditors assess the severity of IT security incident reports. These reports may contain details such as unauthorized access, data breaches, or system vulnerabilities.

To make this work, auditors need good training data, such as historical IT security reports that are tagged with risk ratings (high, medium, or low). By applying the algorithm to new reports, auditors can categorize incidents by their severity and prioritize high-risk issues more effectively.

Using the Python scikit-learn library, auditors can train the machine learning model on 70% of the historical data and test it for accuracy on the other 30%. Auditors also can apply a clustering algorithm to group multiple documents.

Generative I

With generative AI, chatbots and virtual agents can deliver personalized responses. Tools such as ChatGPT, Copilot, and Gemini can instantly summarize themes from PDFs, Google Docs, and Office Docs.

The right prompt will enable these tools to focus specifically on risk, compliance, or security. That can help auditors transform dense information into prioritized remediation steps and decision-making guides for executives.

Beyond these tasks, auditors can use large language models to extract themes from documents at scale. For example, the Python LangChain library integrates with models such as ChatGPT and can extract topics and themes from documents.

To identify these themes, auditors must create a prompt such as:

You are a document assistant, and I would like to retrieve the top themes/topics from a set of incident reports and security audit findings. Highlight topics specific to risk, compliance, and security. Focus on identifying recurring vulnerabilities, compliance violations, and noncompliance with data protection regulations.

Data-Driven udits

Unstructured data is a goldmine for internal auditing. When analyzed well, it can reveal recurring issues, flag emerging risks, and help practitioners plan smarter and more targeted audits — even if they only have basic programming skills.

As a result, audits become faster, more proactive, and more data-driven. By tapping into unstructured data, internal auditors can turn information into actionable insights that improve risk management and decision-making.

shwathama Rajendran is a data analytics lead at Stripe in Boston.

Surprises in Organisations and the Internal udit Response Reflections from the RPG nnual C E Meet 2026

In today's dynamic business environment, organisational failures and disruptions are rarely completely unexpected. More often, subtle early warning signals exist long before issues escalate. Recognising these signals and responding proactively is increasingly becoming a critical responsibility of the Internal Audit (IA) function.

Against this backdrop, the Assurance & Internal Audit Department at RPG Enterprises hosted its Annual CAE Meet on April 17, 2026, on the theme "Surprises in Organisations and the Internal Audit Response." The conference was presided over by Mr. Suresh Mathew, Executive Director – Chairman's Office, and Mr. Anirban Dasgupta, Group Head – Assurance & Internal Audit. The event brought together industry leaders, Chief Audit Executives, and consulting professionals to discuss emerging organisational risks and the evolving role of Internal Audit.

A recurring theme during the discussions was the growing gap between rapid business expansion and the maturity of processes and controls. Mr. Anthony Crasto, President – Assurance at Deloitte South Asia, highlighted the need for auditors to develop greater professional scepticism and adopt a holistic perspective while assessing risks. Ms. Ritu Sethi, CAE at Generali Central Insurance, observed that recurring SOP deviations, manual approvals, and business workarounds should be viewed as indicators of deeper systemic concerns.

The conference also explored situations where risk management frameworks appear robust on paper but fail in practice. Mr. Chetan Thakar, Head of Audit & Risk Management at JSW Ports & Paints, stressed the importance of tracking non-compliances as indicators of emerging risks, while Mr. Shaival Nanavaty, Partner at RSM India, emphasised the importance of stronger business understanding within Internal Audit teams.

The importance of culture and behaviour as risk indicators also featured prominently. Mr. Uday Pawar, Senior Vice President at Kalpataru Projects International Limited, spoke about the need for auditors to "audit people" and understand organisational behaviour, not just processes and controls. Similarly, Mr. Pankaj Kumar, CAE at CEAT Ltd., highlighted the importance of creating systems that are more process-driven and less dependent on individuals.

Further, Mr. Shyamsukha Jhahanwijha, Partner at KPMG, emphasised the need for auditors to question inconsistencies and investigate uncomfortable issues. Mr. Sunil Bhadu, Partner & Head – Governance, Risk and Controls (GRC) at PwC, stressed that controls should remain simple, practical, and understandable to ensure effectiveness.

About RPG Enterprises
RPG Enterprises, established in 1979, is a Rs 49,000 crores diversified business group with interests across Infrastructure, Tyres, Pharma, IT, Specialty, and emerging innovation-led technology businesses.

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

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