ISACA
Bangalore Chapter

Q2 - 2025 ISSUE

InfocITy Auditor

ISACA Bangalore Chapter - News Letter

ISACA
Bangalore Chapter

Executive Committee - 2024-2025

President
Ms. S Vijayavanitha

Vice President
Mr. Deepak GB

Secretary
Ms. Suma KV

Treasurer
Mr. T R Rajesh

Director - Programs
Mr. Narasimhan Elangovan

Director - Membership
Virupakshi HM

Director - SIG
Gaurav Mukhija

Director - Research & GRA
Mr. Rama Prasad BK

Director - Academic Relations
Mr. Sampatkumar Krishnasamy

Director /Coordinator - CISM, CRISC & ITCA
Ms. Lalitha Satheesh

Director/Coordinator - CISA, CGEIT & CDPSE
Mr. Naveenkumar MS

Director - Marketing
CA. Chandra Prakash Jain

Director - Web Services
Mr. Raghava Rachuri

Director - Newsletter
Anand D

Immediate Past President
Mr. Rajasekharan K R

CONTENTS

ISACA Bangalore Chapter

InfocITy Auditor

Q2 - 2025

From The Desk Of The President

Dear Members,

I hope this message finds you well! Our ISACA Bangalore Chapter continues to thrive, now boasting over 2535 members. This growth truly reflects the trust and confidence you place in us, and we are committed to upholding it. We've actively conducted various CPE sessions, including popular ones like "The Journey to Future Technology" and "Beyond Compliance: VAPT for Real Security Maturity," thanks to your enthusiastic participation.

A major highlight was our successful involvement in the Internal Security Summit at SAP Labs Bangalore. With over 200 attendees, our booth was a vibrant hub, allowing us to connect with professionals and showcase our training and certification programs, reinforcing the value of ISACA's offerings.

We were also honored to represent India at the inaugural ISACA Asia Virtual Conference. Our session on "Artificial Intelligence in India's Sustainable Urban Development" was a standout, receiving the highest "Excellent" rating. This success further elevates our engagement with the professional community.

Looking ahead, registration has begun for our 28th Annual Karnataka Conference 2025, themed "Resilience by Design: Embedding Security, Audit & Governance in AI-Driven Ecosystems." We've already seen an incredible response with 300 registrations, a historic first for our chapter! As a special thank you, the first 75 registrants will receive complimentary online training on "AI for Information Security Governance & Risk Management Professionals," offering 3 valuable CPE Credits.

The Board of Directors and I are excited to see you in person at the conference. We also extend our sincere gratitude to all our sponsors for their continuous support. Your contributions are deeply appreciated! Let's continue building a strong, secure, and collaborative professional community together.

Best Regards,
VIJAYAVANITHA, CISA, CIA, MBA, M Com

Message From the Vice President

Dear Members,

As we prepare to release this special edition of our chapter newsletter during the much-anticipated Annual Karnataka Conference, I take immense pride in reflecting on our recent achievements and the momentum we continue to build together.

Over the past months, the ISACA Bangalore Chapter has hosted a series of impactful CPE sessions, both in-person and virtual, featuring industry experts across diverse domains of cybersecurity, risk management, emerging technologies, and governance. These sessions not only enabled our members to upskill but also fostered vibrant knowledge-sharing among peers. The consistently strong participation is a testament to our community's passion for continuous learning.

Another point of pride, Bangalore continues to hold the top spot nationally in terms of ISACA membership. This is a reflection of the trust and value our members place in the chapter's offerings, and it further strengthens our commitment to serve you with relevant, engaging, and high-quality programs.

As we unveil this edition during our Annual Conference, which promises to be one of the largest and most dynamic events yet, I invite you all to take a moment to celebrate the collective accomplishments of our community. Each article, update, and highlight in this newsletter echoes the spirit of collaboration and forward-thinking that defines our chapter.

I also encourage all of you to **be active participants** in the chapter's ongoing activities. Whether it's attending events, contributing thought leadership, volunteering, or even stepping into leadership roles, your involvement is what drives the chapter forward. We especially welcome members who are keen to support **chapter operations**, helping us expand our reach and impact.

Together, let's continue to build a stronger, more connected, and future-ready ISACA community. Thank you for being an integral part of our journey. Let's continue to lead, learn, and grow together.

Warm Regards,
DEEPAK BHASKARAN

Message From Secretary

Dear Esteemed Members of ISACA Bangalore Chapter,

As we reflect on our shared journey within the ISACA Bangalore Chapter, I am filled with immense pride and gratitude for what we have accomplished together. Our chapter stands as a beacon of professional excellence, thought leadership, and unwavering commitment to advancing the fields of IT governance, risk management, cybersecurity, and audit.

Every milestone we achieve is much more than just a statistic—it is a story of dedication, innovation, and the collaborative spirit that defines our community. From industry-leading conferences and insightful knowledge sessions to hands-on workshops and impactful outreach, your participation and passion have been the cornerstone of our success.

But our journey does not stop here. As the digital landscape evolves at a rapid pace, so do the opportunities and challenges before us. I encourage each of you to remain engaged—attend our events, share your expertise, and mentor the next generation of professionals. Let us harness our collective strengths to set new benchmarks and lead the way in building a secure and resilient digital future.

Remember, each of you is a vital part of the ISACA Bangalore Chapter's legacy and future. Your ideas matter, your contributions drive change, and together, there is no limit to what we can achieve.

Let's continue to inspire, innovate, and elevate our chapter—together.

With sincere appreciation and optimism,
SUMA K V

Renewal of ISACA Membership for the year 2025

Warm Greetings from ISACA Bangalore Chapter!!!

We thank you for your continued support and commitment to professional excellence by earning one or more of ISACA Certifications.

Use your ISACA® membership and ISACA certification(s) as the platform for your growth by utilizing the opportunities for professional development. As you would have experienced, your ISACA membership and certification(s) increase your advancement opportunities by keeping you informed of standards and good practices in the fields that matter most to you and providing access to leading edge research and knowledge through Journals, Webinars, Blogs, ISACA e-library, local chapter events and many more.

Also, you are aware ISACA Bangalore Chapter provides significant benefits and local networking opportunities to its members. The chapter has been in the forefront and served its members in their quest for acquiring professional knowledge by conducting regular CPE Sessions, Webinars, Conferences and other professional development programs. At the chapter it is our endeavor to bring to the table the most relevant of the current topics and encourage active participation of members.

In case you need any assistance, please do not hesitate to reach out to Chapter Office at chapter@isacabangalore.org

The ISACA Bangalore Chapter has been successfully conducting **quarterly review classes** for globally recognized certifications - **CISA**, **CISM**, **CRISC**, **CGEIT** and **CDPSE -** providing high-quality, exam-focused training to professionals in the fields of audit, risk, cybersecurity, governance, and privacy. These programs are led by **experienced, certified trainers** who bring real-world expertise and domain insights, ensuring deep conceptual understanding and practical application. Each course is aligned with the **latest ISACA exam content**, covering key domains, and exam strategies. The sessions are tailored for **working professionals**, delivered on **weekends** in **online formats** for maximum accessibility. Participants consistently praise the interactive format, clarity of instruction, and real-time examples that bridge theory with practice. Over the past quarters, these classes have enabled hundreds of professionals to achieve certification success and career advancement. The review programs also foster peer learning and active engagement through Q&As and follow-up support. Designed not just to pass exams, but to build future-ready GRC leaders, these sessions are now widely regarded as a preferred training pathway across industries. ISACA Bangalore's commitment to **continuous professional development** and global best practices shines through every batch. Registration details and batch schedules are regularly updated on the chapter's official platforms.

Registration Link:
Members (with mandatory member id) : https://isacabc.mojo.page/online-review-classes-2025-members
Non-Members : https://isacabc.mojo.page/online-review-classes-2025-non-members

Recap of Chapter Programs in Q2, 2025

CPE Sessions From April 2025 to June 2025 :

1. **Topic : "The Journey to Future Technology"**
   Speaker : Mr. TR Rajesh
   Date : 31-May-2025 (Saturday) Time : 5:30 PM - 7:30 PM IST
   Venue : ISACA Bangalore Chapter Office - Physical Session
   Free Attendance : 2 CPE Credits offered

About the Speaker : Mr. TR Rajesh

He is a DSCI certified Strategist, cyber security professional with 27+ Years of experience in information security, Cloud, AI/ML, risk management, policy, data privacy, regulatory requirements, Transition & Transformation, internal & external audits & reviews, Third party vendor security assessments, and Security Operations Centre management.

Rajesh is a Mentor, authorized Trainer, and speaker in many forums and institutions.

2. **Topic : "Implementing Foundational Cybersecurity for DoD Contractors Using CMMC Levels 1 & 2 and NIST SP 800-171"**
   Speaker : Mr. Vijay Reddy - Cyber Security Head at DQS
   Date : 14-June-2025 (Saturday) Time : 5:30 PM - 7:30 PM IST
   Venue : ISACA Bangalore Chapter Office - Physical Session
   Free Attendance : 2 CPE Credits offered

Session Overview:

This webinar provides a practical overview of how DoD contractors can implement foundational Cybersecurity measures in alignment with CMMC Levels 1 and 2, leveraging the control requirements of NIST SP 800-171. Participants will learn how to interpret and apply security controls across key domains such as access control, incident response, and system integrity. The session will also cover strategies for preparing System Security Plans (SSPs), managing POA&Ms, and building assessment readiness. Designed for contractors across the Defense Industrial Base (DIB), this webinar equips attendees with actionable steps to meet current DoD Cybersecurity compliance expectations

Key Learning Objectives:

- **Describe the structure and intent of the CMMC 2.0 framework**, with specific focus on the requirements for Levels 1 and 2 applicable to DoD contractors.
- Interpret **an implement NIST SP 800-171 security controls** across 14 control families to meet the technical and procedural requirements of CMMC Level 2.

- **Develop and maintain a System Security Plan (SSP) and POA&M**, including understanding their purpose, required content, and audit-readiness best practices
- **Describe the structure and intent of the CMMC 2.0 framework**, with specific focus on the requirements for Levels 1 and 2 applicable to DoD contractors.
- **Interpret and implement NIST SP 800-171 security controls** across 14 control families to meet the technical and procedural requirements of CMMC Level 2.
- **Develop and maintain a System Security Plan (SSP) and POA&M**, including understanding their purpose, required content, and audit-readiness best practices.
- **Conduct a gap assessment to evaluate current cybersecurity posture**, identify deficiencies, and create a prioritized remediation roadmap aligned with CMMC controls.
- **Prepare for CMMC assessments** by collecting appropriate evidence, aligning documentation with assessor expectations, and avoiding common compliance pitfalls.

About the Speaker : Mr. Vijay Reddy

A seasoned Enterprise Risk and Cybersecurity Leader with over two decades of global experience in aligning cybersecurity initiatives with business objectives across diverse industry sectors. Proven expertise in leading security architecture, governance, and compliance programs for top-tier firms such as TCS, Accenture, Virtusa, and AVL. Recognized for translating complex cybersecurity requirements into actionable strategies using a risk-based, standards-compliant framework. Combines deep technical acumen with business insight to drive secure digital transformation.

Key Areas of Expertise

- CMMC Audit and Implementation& Readiness Assessment
- Integration of Cybersecurity Frameworks (NIST, ISO 27001, CIS Controls)
- Enterprise Risk Assessment & Compliance Roadmaps
- Regulatory Compliance Across Healthcare, Finance, and Government Domains

3. Topic : "Beyond Complaince : VAPT for Real Security Maturity"
Speakers : Mr. Falgun M Rathod
Date : 28-June-2025 (Saturday) Time : 5:30 PM - 7:30 PM IST
Venue / Platform : Web-based ONLINE Session via Zoom Webinar Platform
Free Attendance : 2 CPE Credits offered

Session Overview:

In today's rapidly evolving threat landscape, organizations can no longer afford to treat Vulnerability Assessment and Penetration Testing (VAPT) as a mere compliance checkbox. While regulatory frameworks mandate periodic assessments, these often fall short of uncovering deeper, contextual security gaps that adversaries exploit.

This webinar explores a transformative approach to VAPT—shifting the focus from baseline compliance to achieving real security maturity. Effective VAPT must be continuous, risk-based, and aligned with business-

critical assets and processes. By embedding threat modeling, contextual risk assessment, and adversary simulation into the VAPT lifecycle, organizations can identify not only technical vulnerabilities but also systemic weaknesses in security architecture and response readiness. Through real-world use cases and a maturity-driven VAPT framework, the webinar highlights how organizations can elevate their cybersecurity posture.

Key Learning Objectives:

By attending this session, Participants will be able to Learn Vulnerability Assessment across different types of IT Infrastructure, Penetration Testing Activities & Advanced Exploits

About the Speaker : Mr. Falgun M Rathod

He is the Managing Director and CTO of Cyber Octet Pvt. Ltd., a company recognized among the Top 25 Promising Cyber Security Companies in India by Silicon India Magazine. He has over 16 years of experience in information security and cybercrime investigation. He serves as a consultant to state and national security agencies within the government sector and holds multiple certifications, including ISO/IEC 27001:2022 Lead Auditor, ISO 22301 Internal Auditor, Lean Six Sigma Green Belt, Project Management Essentials, ITSM Associate, and ISO/IEC 42001:2023 AI Management System Lead Auditor. He is also the author of two Amazon bestselling books and has been listed among the Top Ten Certified Ethical Hackers in India (Silicon India) and Top Ten Cyber Cops in India (India Today). His credentials include training and certifications from the United Nations and the U.S. Department of Homeland Security, including OPSEC and ICS-CERT programs. He is a mentor at BugsXploration, chapter leader at OWASP, and a member of several international cyber threat and security forums. He has been a keynote speaker at HACKATHON 2012 and a frequent guest at academic events and faculty development programs.

He was also adjudged as the “Winner of Times Man of The Year in Cyber Security Education in 2023”

Other Supported Events:

- ISACA Asia Virtual Conference 2025, Co-hosted by the Bangalore and Singapore Chapters, on 6th June 2025 (8.00 AM- 1.00 PM IST.)
- This Online event Covered Key Regional Themes Includes CISO Leadership, data & AI Governance and Cyber resilience.
- Free Attendance: 05 CPE Credits Offered
- Expect: Key notes, Expert Panels with Asian ISACA Leaders, Country specific Cyber security insights etc.

The Hidden Costs of GRC Silos - And Why It's Time to Break Them Down

ABOUT WRITER :

The writer is the Practice Head at CyRAACS with extensive experience in cybersecurity, risk management, and compliance and is known for her practical insights on integrated risk and compliance ecosystems. She holds certifications including CISSP, CISA, and CIPM.

In today's ever growing technology and compliance-driven world, organizations face a unique challenge: their governance risk and compliance (GRC) functions though vital for operations operate in silos. The compliances and governance requirements across legal, audit, risk, information security, and operations define their individual framework and objectives with its own tools, assessment formats, and reporting mechanisms. These silos are not only inefficient; they do not provide the integrated view for the management for business decision making.

Overall, the GRC structures in banks or IT services organizations may appear organized with a well-defined charter and internal trackers. Though the real challenges lie in redundancies across the functions, miscommunication, and an incomplete understanding of organizational risk. For Example: The **privacy compliance function** maps GDPR and ISO 27701 requirements in spreadsheets, while the **information security team** handles ISO 27001 audits through another GRC platform. This results in duplicated efforts in evidence collection, with different control interpretations for the same systems. Each team manages their control framework and presents their fragmented observations impacting the overall decision making for the organization.

The cost of the GRC silos though aren't always visible on balance sheets exist in every delayed audit, duplicated control, and missed insight:

- **Audit Fatigue**: Teams face repetitive audits and artefact collection requests across internal audit, client audits, and certification reviews.
- **Inconsistent Risk Assessment and Treatment**: Due to multiple fragmented frameworks within the teams, there are inconsistent assessment and reporting of the risks identified. For example: Vendor Due Diligence team may flag a vendor as low risk due to SLA metrics reported, while another escalates the same vendor for poor encryption controls.
- **Fragmented Reporting**: Risk reports to the board lack cohesion as each function presents its own dashboards, with no cross-functional correlation.

Organizations have now realized the risk and impact of the GRC Silos and are working towards building unified GRC ecosystems which is integrated and designed for strategic decision-making.

The unified GRC ecosystem provides:

- A single control and risk taxonomy across audit, cyber, risk, and compliance.
- AI and automation powering control validation, risk scoring, and document mapping in real time.

- Adaptive framework to swiftly align to changing regulations, evolving threats, or new business geographies.

COMPASS – Supporting the adoption of the unified GRC ecosystem:

The progressive GRC ecosystem not only requires awareness, it also needs an intelligent, purpose-built platform that centralizes efforts and promotes collaboration across governance functions. COMPASS by CyRAACS is specifically designed to address the requirement.

Take an example of audit fatigue. Instead of repetitive documentation across compliance functions, COMPASS offers centralized control libraries and snapshots of control changes, which significantly reduces redundancy and enables smoother responses to client, internal, or regulatory audits. When organizations face inconsistent risk ratings across departments, COMPASS provides an integrated risk and control framework, so risk ownership, treatment, and assessments remain aligned—regardless of who is initiating the assessment.

COMPASS enables cross-functional teams to view linked risks, issues, and controls to empower real-time risk awareness and timely resolution of the issues identified. This eliminates the delays that often stem from siloed visibility.

Perhaps most critically, COMPASS renovates fragmented reporting into a holistic views. Instead of isolated dashboards per function, the platform consolidates data into a single view to be consumed by the CISO of the organization, mapping risks to business functions, tracking control performance over time, and identifying overlaps in obligations across frameworks like ISO 27001, SOC 2, RBI, and GDPR.

From continuous control sustenance to issue tracking, third-party assessments, and snapshot-driven governance, the platform eliminates silos and enables organizations to operate with clarity, precision, and foresight.

In a world where regulatory complexity, cyber threats, and reputational risks intersect daily, breaking down GRC silos and adopting the GRC ecosystem strategically.

Cyber Resilience doesn't come from adding more frameworks or tools. It comes from clarity, connection, and context. The future of GRC is not about managing frameworks in isolation. It's about building connected compliance ecosystems and leading organizations are already making that shift.

BREAK THE SILOS. UNIFY THE VISION. POWER RESILIENT GROWTH.

Identity is the New Perimeter : Auditing IAM in an Age of Zero Trust

By : Tharun Krishnamoorthy

Introduction: From Firewalls to Fingerprints

Once upon a time, enterprise security depended on clear perimeters - firewalls, VPNs, and data centers. If you were inside the network, you were trusted. If you were outside, you weren't.

Fast forward to 2025: the perimeter is gone. Cloud-native architectures, hybrid work, SaaS sprawl, API integrations, and third-party contractors have reshaped the landscape. Trust can no longer be assigned based on location or device. Instead, identity has become the core control plane for access, authorization, and assurance.

In a Zero Trust model - where no entity is implicitly trusted - Identity and Access Management (IAM) is the front line of defense. For auditors, this is both a challenge and an opportunity. Traditional IAM reviews focused on user provisioning and password complexity. Modern IAM audits must now cover federated identity, dynamic entitlements, Just-In-Time access, privileged identity management (PIM), and continuous verification.

Why IAM Is Core to Zero Trust

Zero Trust is not a single product or policy - it's a security philosophy that assumes breach, enforces least privilege, and demands continuous validation. Identity is central to this model for several reasons:

- Users and devices are everywhere: Remote work, BYOD, and cloud services make perimeter-based access obsolete.
- Access is dynamic: Employees change roles, projects evolve, and contractors onboard and offboard frequently.
- Threat actors exploit identity: 80% of breaches today involve compromised credentials or privilege escalation (source: Verizon DBIR).
- Compliance mandates are rising: Regulations like GDPR, HIPAA, and SOX increasingly require fine-grained access controls and audit trails. In this context, auditing IAM becomes a strategic lever—not just for compliance, but for operational resilience.

What Auditors Should Look For: IAM Control Areas

A modern IAM audit must evaluate more than onboarding/offboarding checklists. Here's what to examine:

1. **Identity Governance and Administration (IGA)**
   - Are there centralized directories (e.g., Azure AD, Okta) managing identities across cloud and on-prem systems?
   - Is there RBAC or ABAC (attribute-based access control)?
   - Are entitlements reviewed periodically, and are exceptions tracked?
   - Is there separation of duties (SoD) logic embedded into provisioning?
2. **Authentication and Authorization**
   - Are MFA (multi-factor authentication) policies enforced across critical assets?
   - Are SSO (Single Sign-On) systems in use, and is federated identity configured securely?
   - Are token lifetimes and session timeouts aligned with risk?
3. **Privileged Access Management (PAM/PIM)**
   - How are admin accounts governed?
   - Is Just-In-Time access enabled for sensitive roles?
   - Are shared accounts eliminated or managed with vaults and session recording?
4. **Joiner-Mover-Leaver Processes**
   - Is provisioning automated via HR triggers?
   - Are access reviews triggered for department transfers?
   - Are leaver accounts deactivated in real time?

5. **Access Reviews and Certifications**

- Are managers certifying access periodically?
- Are toxic combinations flagged (e.g., finance + approval access)?
- Can auditors trace access requests, approvals, and revocations end-to-end?

Case Example: IAM Audit at a Cloud-Native Fintech

At a digital-first fintech firm, an internal audit team discovered dormant admin accounts tied to an old project. These accounts still had API keys with access to customer PII.

The audit focused on:

- Incomplete de-provisioning
- Lack of JIT or time-bound access
- Manual review cycles that failed to surface low-risk accounts

After implementing:

- Azure PIM with just-in-time access
- Automated leaver workflows from Workday to AD
- Weekly anomaly detection dashboards

The company reduced its privileged account footprint by 60% and gained real-time visibility into access risks.

Modern IAM Tools Auditors Should Be Familiar With

1. Cloud Identity Platforms: Azure AD, Okta, Google Identity
2. Access Review Tools: Saviynt, SailPoint, OneIdentity
3. PAM Solutions: CyberArk, HashiCorp Vault, BeyondTrust
4. IAM-as-Code: Terraform + Open Policy Agent (OPA)
5. SIEM + UEBA: Identity-based anomaly detection via Splunk, Microsoft Sentinel, or CrowdStrike

Key Audit Questions to Ask

- Do we have a current identity inventory across apps, cloud, and on-prem?
- Can we trace who accessed what, when, and why?
- Are access rights aligned with job roles and revoked on exit?
- Are privileged accounts governed with time-bound access and monitoring?
- Is IAM policy enforcement consistent across environments?

IAM Metrics to Track

Metric	Why It Matters
% of users with privileged access	Indicates potential lateral movement risk
% of inactive accounts over 90 days	Dormant access = breach opportunity
Mean time to deprovision	Reflects process maturity
% of SSO-enabled apps	Higher = better access control
Number of access exceptions	Should be monitored and justified

IAM Audit in a Zero Trust World: A Checklist

- Centralized identity provider in place
- MFA enforced across critical apps
- RBAC or ABAC model adopted
- Periodic access review cycles executed
- Privileged accounts governed via JIT or vaults
- Shadow IT and shadow access discovery in place
- IAM aligned with Zero Trust principles across data, device, and network layers

Conclusion : Identity is the New Firewall

In a world where data lives in the cloud, users work from anywhere, and attackers operate at machine speed, identity becomes the single source of truth. Auditors must evolve from checkbox provisioning reviews to risk-centric IAM assurance - backed by data, automation, and context. If the perimeter has dissolved, then IAM is the new perimeter, and assurance must be baked into every identity interaction. Let audit not be the last line of defense - but the first signal of insight.

Operationalising AI Accountability : The Auditor's Blueprint for 2025 and Beyond

By : Tharun Krishnamoorthy

Introduction: Why AI Accountability Now?

Artificial Intelligence (AI) is embedded in core decision-making systems across every industry. It determines who gets hired, who qualifies for a loan, how health conditions are triaged, and what risks are flagged in cybersecurity systems. While this has enhanced productivity and outcomes, it has also created significant governance gaps. These systems are often black boxes—opaque, complex, and built on data pipelines that can reinforce societal biases.

AI accountability, therefore, is the foundation for the ethical deployment of AI. It ensures that organisations not only comply with regulations but also uphold their commitments to transparency, fairness, and trust. Without mechanisms to audit and govern AI systems, businesses face a mounting risk of reputational harm, litigation, and systemic failures.

As organisations embrace AI, internal audit functions must move beyond traditional checklists. The risks posed by AI are dynamic, interdependent, and require continuous oversight. This article outlines the frameworks, strategies, and tools available to auditors seeking to operationalise AI accountability in 2025 and beyond.

Understanding AI Risk: Beyond Traditional ITGC

Unlike traditional systems, AI systems are trained on data rather than explicitly programmed. This means they inherit patterns from historical datasets, which can include embedded biases or unrepresentative samples. Risks like model drift, explainability gaps, and adversarial attacks are common.

For example, a loan approval AI model trained on urban data may perform poorly in rural settings. Without ongoing monitoring, these performance degradations can go unnoticed. Additionally, deep learning models are often 'black boxes' - even developers can't explain how specific decisions are made. This violates principles of accountability and legal requirements such as GDPR's Article 22.

The growing use of Large Language Models (LLMs) and foundation models introduces new risks: hallucination, prompt injection, and unintended inferences. These cannot be captured through standard access or change management controls. A new audit mindset is required - one that evaluates AI performance over time and its alignment with intended objectives.

Frameworks for Assurance: NIST AI RMF and ISO 42001

Global standards have emerged to guide AI assurance:

NIST AI Risk Management Framework (AI RMF)

Launched in 2023, this framework outlines a lifecycle approach to managing AI risks. It encourages organisations to map AI systems, measure risk, manage controls, and establish governance. Its modular structure enables internal audit teams to align scope with maturity.

ISO/IEC 42001:2023

The first international AI Management System Standard. ISO 42001 defines governance controls across data quality, testing protocols, documentation, and continuous monitoring. For audit teams, it offers a roadmap to evaluate governance practices, data lineage, model retraining procedures, and risk registers.

Together, these frameworks enable audit functions to establish a baseline maturity, identify gaps, and provide a scalable model for assurance.

The Auditor's Expanded Role in 2025

Auditors must now work across the AI lifecycle - from data ingestion to deployment. Their key roles include:

- **Model Inventory Creation**: Maintain a live register of all AI systems in use across the organisation - internal and third-party.
- **Bias and Fairness Reviews**: Examine model inputs, labels, and outputs for disproportionate outcomes across gender, race, age, or geography.
- **Lifecycle Monitoring**: Evaluate how models are maintained—e.g., frequency of drift detection, retraining triggers, and performance benchmarks.
- **Explainability Testing**: Use tools like SHAP (Shapley Additive Explanations), LIME (Local Interpretable Model-agnostic Explanations), and Counterfactuals to assess how models arrive at decisions.
- **Regulatory Readiness**: Review if documentation meets the requirements of regulatory frameworks like the EU AI Act and India's Digital Personal Data Protection Act.

Collaborating with data science teams is essential. Auditors don't need to build models - but must ask smarter questions:

- What assumptions is this model based on?
- What controls exist if it fails?
- Who monitors bias, and how often?

Tools like EvidentlyAI and Aequitas help visualise drift, bias, and feature distribution shifts - critical for non-technical audit use cases.

Real-World Examples & Metrics

Amazon's Recruitment Model (2018)

An internal tool trained on historical resumes penalised resumes with the word "women." Bias was learned from the male-dominated past hiring data. The model was shut down after internal audits exposed the issue.

Apple Card Bias Case (2019)

Goldman Sachs' Apple Card was accused of offering drastically lower credit limits to women than men with similar credit profiles. The New York State Department of Financial Services launched an investigation. The lack of explainability worsened the public response.

Zillow's iBuying Algorithm Failure (2021)

Zillow used AI to forecast house prices and guide purchase decisions. The model's over-optimism and failure to account for local volatility caused $300M in losses and mass layoffs.

Key Audit Metrics:

Metric	What It Measures
Accuracy / Recall	Model performance and correctness
Bias Parity Ratio	Outcome fairness across groups

Feature Drift	Changes in input distribution over time
SHAP Value Spread	Feature importance consistency
Retraining Frequency	Model refresh cycle and performance decay risk
Incident Reports	Escalated edge cases or anomalies post-deployment

Audit as Enabler: Moving from Reactive to Proactive

The biggest shift auditors must make is **from snapshot assurance to continuous engagement**. AI systems don't sit still—they evolve as data changes, behaviours shift, and regulations evolve.

Audit's role is to embed questions into each lifecycle checkpoint:

- During design : "Is this model even needed?"
- During development : "Are data labels accurate and unbiased?"
- During testing : "What happens at model failure thresholds?"
- During deployment : "Who owns the retraining logic?"
- During operations : "Is this model still working as intended?"

Continuous assurance means partnering with GRC, IT, data science, and legal teams. The audit report is not the end—it's the starting point for better governance and trust-building.

Conclusion: The Blueprint Going Forward

AI accountability is not a future concept - it's a current necessity. By adopting frameworks like NIST AI RMF and ISO 42001, building continuous monitoring processes, and integrating audit early in the lifecycle, we can ensure AI systems serve organisational goals **without compromising ethics or safety**.

As auditors, we must evolve into **strategic enablers** - bringing together technical, ethical, and business dimensions. The organisations that do this well will not only pass audits - they will win trust, attract talent, and lead the AI-powered future.

References & Tools

- *NIST AI Risk Management Framework: https://www.nist.gov/itl/ai-risk-management-framework*
- *ISO 42001 Standard Overview: https://www.iso.org/standard/81228.html*
- *SHAP: https://github.com/slundberg/shap*
- *LIME: https://github.com/marcotcr/lime*
- *Aequitas Bias Audit Toolkit: https://github.com/dssg/aequitas*
- *AI for Drift/Bias: https://evidentlyai.com/*
- *EU AI Act (Summary): https://artificialintelligenceact.eu/*
- *India Digital Personal Data Protection Act (2023) : https://www.meity.gov.in/*

ISACA at the Internal Security Summit - SAP Labs | May 20, 2025

We were honored to participate in the **Internal Security Summit** hosted by **SAP Labs** on **May 20, 2025**, at the **Bengaluru Marriott Hotel, Whitefield**.

Our presence at the summit highlighted the **transformative value ISACA brings** to professionals in the fields of **IT Governance, Cybersecurity, and Risk Management**.

We were thrilled by the **enthusiastic participation from the SAP team** at our booth. Engaging conversations, insightful exchanges, and the distribution of curated brochures allowed us to showcase how ISACA's globally recognized certifications and training programs—**CISA, CISM, CRISC, CDPSE, and CGEIT**—can significantly elevate professional growth and organizational resilience.

We thank SAP Labs for the opportunity and look forward to continued collaboration in building a secure and well-governed digital future.

Glimpses from the Free ISACA Introductory Session and CPE Session Held on May 31, 2025 at the Chapter Office

India Ranks #1 in Excellence - ISACA Asia Virtual Conference (June 6, 2025) Feedback Highlights!

ISACA Asia Virtual Conference held on June 6, 2025, was a grand success! This year marked a significant milestone as it was the **first time ever that the ISACA Bangalore Chapter partnered with the ISACA Singapore Chapter** for this conference. The event featured regional panels and chapter-specific discussions.

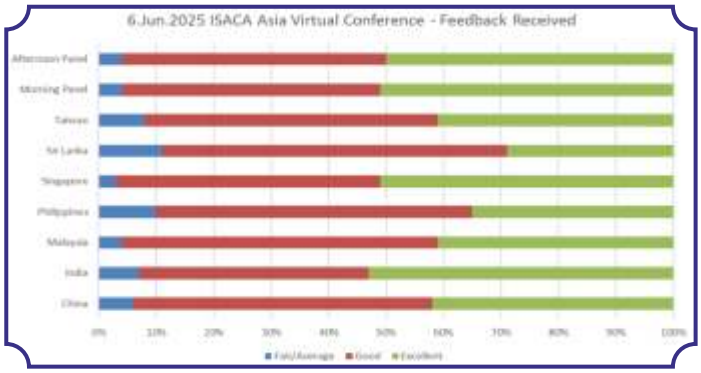
We are incredibly proud to announce that **India, represented by the ISACA Bangalore Chapter, ranked first in overall excellence** based on participant feedback across all sessions! With a leading share of "Excellent" ratings, India stood out in terms of **content quality, speaker insights, and session engagement**—a true reflection of the effort and dedication of our chapter.

Key Highlights from the Feedback:

- India received the highest proportion of "Excellent" ratings, leading across the board.
- Sessions from Malaysia, Taiwan, and the Philippines also received strong positive responses.
- Both the **Morning and Afternoon Panels were highly appreciated** for their expert discussions.
- Common areas of praise included **Identity & Access Management, BPMN frameworks, and Cybersecurity innovation.**

This recognition is a testament to the quality of our programs and the engagement of our community. Congratulations to all involved!

Let's continue raising the bar together!



Snapshots from the CPE Session on June 14, 2025 at the Chapter Office

Alliance University Mentorship Program : A Resounding Success!

The ISACA Bangalore Chapter proudly announces the remarkable success of our inaugural mentorship program with Alliance University. This groundbreaking initiative saw our dedicated ISACA BC mentors volunteer an astounding **280 hours** of their invaluable time from February 2025 to April 2025,, profoundly impacting **over 117 MCA and B.Tech students**.

Under the exceptional leadership of our Academic Relations Director, **Mr. Sampathkumar Krishnasamy**, mentors provided crucial career road mapping, insights into emerging technologies like AI and quantum computing, and fostered interdisciplinary learning.

We also extend immense gratitude to **Alliance University for their excellent coordination**, which was pivotal in making this program a resounding success. This collaboration has truly bridged the academia-industry gap, empowering the next generation of IT and cybersecurity professionals. We extend our deepest gratitude to all mentors for their extraordinary contributions!

Contributions to ISACA Bangalore Chapter Newsletter

Dear Members,

The ISACA Bangalore Chapter Quarterly Newsletter covers the updates on chapter events, technical articles and whitepapers related to the areas of emerging technologies, IT Governance, Audits and Cybersecurity. In this regard, we encourage our chapter members to send your technical articles and whitepapers to us.

You can send your articles / whitepapers to our chapter email address: chapter@isacabangalore.org

Support from ISACA Bangalore Chapter

Website: https://engage.isaca.org/bangalorechapter/home

Chapter Office Address:

Solus Jain Heights
Unit No : B 10, 10th Floor, First Cross, J. C. Road, Bangalore- 560 002.
T: 080-41514331 / 98865 08515

Email: chapter@isacabangalore.org

Telegram Channel: https://t.me/joinchat/AAAAAEt42QAUpWHucyNyJA

LinkedIN: https://www.linkedin.com/company/isacabc/

Facebook: https://www.facebook.com/ISACABC/


protiviti®
Global Business Consulting


tsaaro®
consulting

Greatness is every team working toward a common goal. Winning in spite of cyber threats and overcoming challenges before they happen. It's building for a future that only you can create. Or simply coming home in time for dinner.

However you define greatness, we're here to help you secure your full potential. Our people, partners, products and programs give you the tools and support you need to face any risk. With Optiv in your corner, you can build a stronger and more resilient business.

www.optiv.com

OPTIV

Book Post

Certified Data Privacy Solutions Engineer™

Certified in the Governance of Enterprise IT®

An ISACA® Certification

Certified Information Systems Auditor®

Certified Information Security Manager®

Certified in Risk and Information Systems Control®

CSX Cybersecurity Practitioner®

If undelivered please return to :

ISACA
Bangalore Chapter

Solus Jain Heights, Unit No. : B10, 10th Floor
1st Cross, J C Road, Bangalore- 5600 02.
Ph. : 080-41514331/9886508515
Email: chapter@isacabangalore.org

Printed @ Cauvery Ent. © 22128682

Chapter Reg No : 433/2002-2003