ISACA
Bangalore Chapter

Q3 - 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

Q3 - 2025

From The Desk Of The President

Dear ISACA Bangalore Chapter Members,

As We Near the Close of the 2024-25 Term

I reflect with immense pride and gratitude on our Chapter's remarkable journey this year. Together, we have achieved new milestones, driven innovation, and strengthened our foundation for future growth.

Breaking New Ground

It has been an honour to serve as the **first woman President** of the ISACA Bangalore Chapter-and the only individual to have served **nine consecutive years on the Board** before taking this role in my tenth year. Our membership grew by **20.11% (2,412 →2,897)**, surpassing ISACA Global's 4% (100) target-proof of the trust and value our Chapter delivers.

Collaborations and Knowledge Partnerships

- Partnered with **ISACA Mumbai Chapter** as Knowledge Partner for **SmartTech Asia 2025**.
- **280+ mentoring hours** delivered through our **Alliance University Program**.
- Launched **ISACA Student Groups (ISGs)** at **Presidency** and **Jain Universities**, nurturing future leaders.

Community and Impact

Through our *"Empowering Young Minds"* initiative with **Sparsha Trust**, we enhanced **digital and financial literacy** for youth. Our **SheLeadsTech 2025 (IWD)** registrations **doubled (72 →131)**, and our **AI in Urban Development** session earned a **top "Excellent" global rating**.

Global and National Recognition

- India shone at the **Asia Virtual Conference 2025**, co-hosted with ISACA Singapore.Internationally, our session on AI at the Asia Virtual Conference received the highest 'Excellent' rating among all countries.
- We also set a new precedent by collaborating with the ISACA Mumbai Chapter for Smart Tech Asia 2025.
- **AKC 2025** achieved record engagement: **6,412 member hours (+31%)** and **19 white papers (+171%)**.
- **Alliance University students** made their debut as Masters of Ceremony.

Leadership and Legacy

The **All-India Presidents' Meet**, attended by **ISACA Global CEO Eric Prusch**, strengthened inter-chapter collaboration. We were invited by **IN-SPACe** to help shape **India's first Cybersecurity Framework for the** Indian **Space Sector** - a historic honor.

Digital Transformation and Global Engagement

- **LinkedIn engagement** grew from <100 to **10,000+ impressions per post**.
- Represented India at the **ISACA Global Leadership Summit 2025 (London)**, engaging with leaders from **92 countries**.

Looking Ahead

This year has been one of **firsts** - driven by our collective vision, volunteer energy, and unwavering member trust. As we continue advancing **digital trust and governance excellence**, I extend my deepest gratitude to every member, past and present.

Here's to a stronger, smarter, and more connected ISACA Bangalore Chapter in 2025-26!

Best Regards,

VIJAYAVANITHA, CISA, CIA, MBA, M Com

Message From the Vice President

Dear Members,

As we conclude another remarkable chapter in our journey, I would like to express my heartfelt gratitude to each one of you for making our **Annual Conference** an extraordinary success. The event was truly spectacular - filled with insightful sessions, inspiring discussions, and vibrant participation from professionals across industries. The enthusiasm, collaboration, and commitment displayed by our members, speakers, sponsors, and volunteers made it a memorable milestone for our chapter.

A special note of thanks to the organizing committee and the extended volunteer team for their tireless efforts and meticulous planning. Your dedication and passion exemplify the true spirit of ISACA - a community built on learning, leadership, and collaboration.

I would also like to acknowledge the wonderful participation in our recent **Community Day** initiatives. Your contributions to giving back to society highlight how our chapter continues to create impact beyond professional excellence - by nurturing a sense of social responsibility and togetherness.

As we move forward, let us carry this momentum and continue supporting one another to strengthen our community and foster innovation and growth in our profession.

I also wanted to extend my warmest wishes to you and your families, as we celebrate this joyous season. May this time of togetherness bring light, happiness, and prosperity to your homes and inspire renewed energy in all our endeavors.

With Sincere appreciation and festive greetings,
DEEPAK GB

Message From Secretary

Staying Connected and Driving Digital Trust

Dear ISACA Bangalore Chapter Members,

I hope this message finds you well and thriving in your professional endeavors. As your Chapter Secretary, I am delighted to connect with you through this latest edition of our newsletter, a platform that serves not only to inform but also to strengthen the bonds within our vibrant community.

The pace of change in **digital trust, cybersecurity, and GRC (Governance, Risk, and Compliance)** continues to accelerate, making the work we do more critical than ever. It's inspiring to see the dedication and expertise of our Bangalore Chapter members as we collectively navigate this complex landscape.

This past quarter has been filled with successful events that underscore our commitment to continuous professional development. In particular, our recent major events mentioned below were phenomenal success, thanks to the insightful speakers, engaging discussions, and excellent participation from all of you.

- **Annual Karnataka Conference with Theme: "Resilience by Design: Embedding Security, Audit & Governance in AI Driven Ecosystems" @ TAJ Hotel, Bangalore on 8th & 9th Aug 2025**
- **CAIO Program Training for 3 Days by Corporate Governance Institute by Copenhagen Compliance @ ISACA Bangalore Chapter Office from 29th to 31st Aug'25**
- **In person workshop with the topic "How Secure Are We?" on 20th September 2025**
- **Panel discussion on the topic "Advancements in Space Technology - C5, and National Security " on 27th September 2025**

Looking ahead, we are focused on providing even more value and opportunities. I encourage you to look closely at the upcoming schedule, including:

- **In person CPE sessions scheduled on 25th October 2025@ Taj MG Road, Bangalore**
- **Annual General Meeting scheduled on 25th October 2025 @ Taj MG Road, Bangalore**

The strength of the ISACA Bangalore Chapter lies in the active participation of its members. Beyond attending events, I want to remind you of a few ways you can make the most of your membership and contribute to our success:

- **Volunteer**: We are always seeking enthusiastic volunteers to help with membership outreach and content development. It's an excellent way to expand your network and earn valuable experience.
- **Contribute**: Have a unique insight or a case study in your domain? Consider submitting an article or a technical paper for our next newsletter edition or presenting at a future CPE event.
- **Engage**: Follow our updates on **LinkedIn and our Chapter website** to ensure you don't miss out on timely announcements on all our events.

Thank you for your commitment to excellence and for being a valued member of the ISACA Bangalore Chapter. Let's continue to uphold the highest standards of digital trust together.

Warm Regards,

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 Q3, 2025

CPE Sessions From July 2025 to September 2025 :

1. **Topic : "Over View of Privacy" (Deep Dive into the Privacy Landscape)**
   Speaker : Mr. DS Mahanty
   Date : 05-July-2025 (Saturday) Time : 5:30 PM - 7:30 PM IST
   Venue : Web-based ONLINE Session via Zoom Webinar Platform
   Free Attendance : 2 CPE Credits offered

Session Overview:

An overview of the origins of privacy concerns and their importance. The talk will also cover the stages in the privacy operational life cycle and the relationship between privacy and security.

Key Learning Objectives:

- Introduction to Privacy
- Four Phases of Privacy Operational Life Cycle
- Intersection of Privacy & Security
- Overview of Global Privacy Laws

About the Speaker : Mr. DS Mahanty

He has conducted online training programs for CISSP, CISA for Corporates Like Master Card, Target,Standard Chartered Bank, Deloitte, etc.

2. **Topic : "DevSecOps - A Leadership Perspective"**
   Speaker : Mrs. Ramkumari Iyer
   Date : 12-July-2025 (Saturday) Time : 5:30 PM - 7:30 PM IST
   Venue : Web-based ONLINE Session via Zoom Webinar Platform
   Free Attendance : 2 CPE Credits offered

Key Learning Objectives:

This session is tailored for leaders, focusing on how to:

- **Cultivate a Culture of Shared Security:** Learn strategies to promote seamless collaboration between development, security, and operations teams, fostering collective responsibility for security.
- **Drive Strategic Organizational Change:** Discover how to champion security as a core business priority, effectively allocate resources, and implement robust metrics for continuous improvement in security practices.

- **Lead Proactive Risk Management:** Develop the ability to guide cross-functional teams in adopting forward-thinking risk management and continuous learning methodologies to enhance both organizational resilience and compliance.

About the Esteemed Speaker : Mrs. Ramkumari Iyer

MRS. RAMKUMARI IYER is a distinguished Principal Consultant, DevOps Evangelist, and a prominent thought leader in Network, Cybersecurity, and Information Security. With over 26 years of extensive corporate experience at leading IT firms including IBM, TCS, Wipro, and Infosys, she has held pivotal roles such as CIO/CISO. She is an award-winning professional, recognized with numerous accolades including CIO awards, Infosec Awards, and the prestigious CISO Champion 2025 award, among many others.

3. Topic : "Beyond Compliance : Unleashing the Power of Data Governance for Secure & Smart Enterprises"
Speakers : Dr. Rajan
Date : 01-Aug-2025 (Friday) Time : 5:30 PM - 7:30 PM IST
Venue : Web-based ONLINE Session via Zoom Webinar Platform
Free Attendance : 2 CPE Credits offered

Session Overview:

This session will delve into the fundamentals of information security, the intricacies of PCI DSS 4.0.1, and practical network segmentation strategies through real-world case studies. You'll gain valuable insights into critical controls across all 12 PCI DSS requirements, including access control, vulnerability management, and secure SDLC. Expect hands-on demos, group discussions, and targeted risk analysis to help you align security practices with both compliance and business needs.

Key Learning Objectives:

- Gain a complete understanding of PCI DSS standard implementation strategies.
- Be empowered to contribute to your organization's roadmap for protecting payment data and information security.
- Deepen your knowledge of Data Governance, Cybersecurity, & Privacy.

About the Speaker : Dr. Rajan

DR. RAJAN, Global Head and Vice President at M/s. SISA Infosec. With 27 years of extensive experience across diverse industries and as a Visiting Professor at BITS Pilani, Dr. Rajan has trained over 1000 cybersecurity professionals globally. His expertise spans Business Continuity Management, Information Security Management, Risk Management, Network Security, Payment Security, and more, backed by impressive global certifications including CISA, CEH, and Six Sigma Master Black Belt.

4. A **complimentary online training workshop**! Dive deep into "**AI for Information Security Governance & Risk Management Professionals**" with expert Mr. Narasimhan Elangovan.

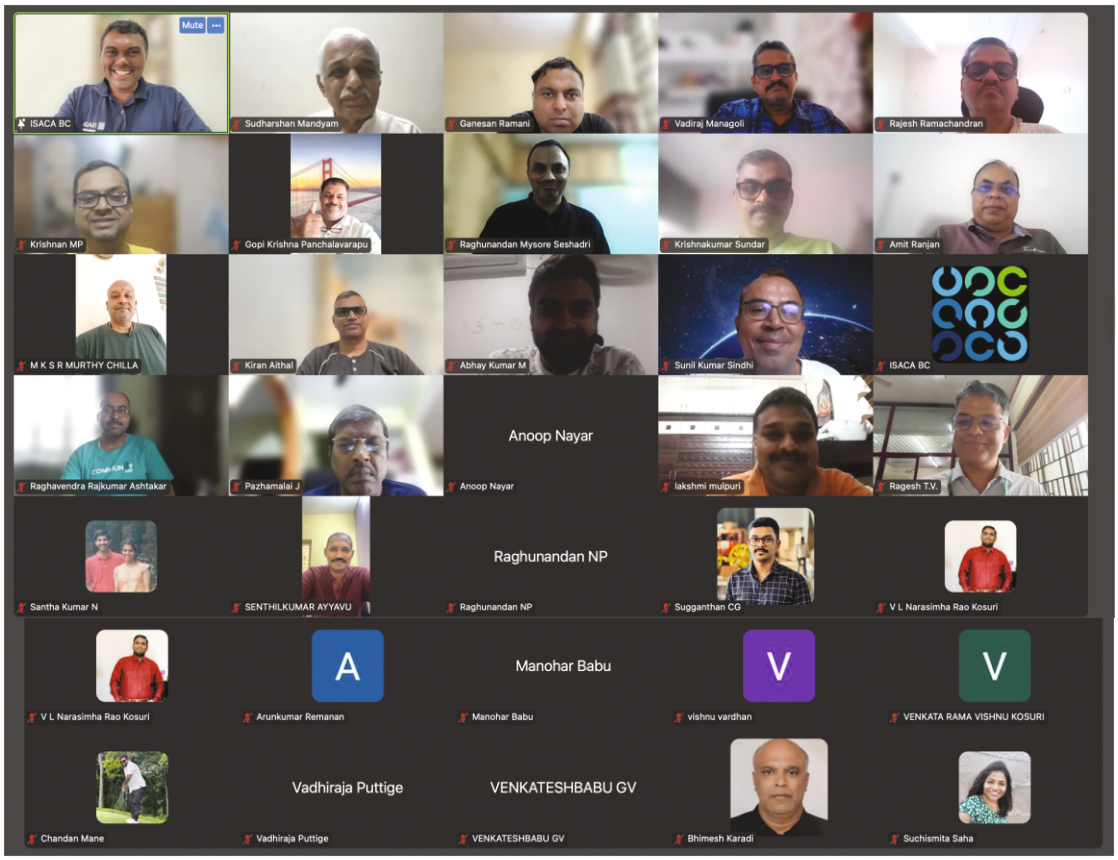
Topic : "AI for Information Security Governance & Risk Management Professionals"
Speakers : Mr. Narasimhan Elangovan
Date : 02-Aug-2025 (Saturday) Time : 10:00 AM - 1:00 PM IST
Venue : Web-based ONLINE Session via Zoom Webinar Platform
Free Attendance : 3 CPE Credits offered

This isn't just theory; it's a practical session focused on applying AI tools in security and audit. You'll gain valuable insights into three key areas:

Key Learning Objectives:

- **AI Governance & Risk:** Learn to build solid AI governance frameworks, assess security risks, and develop responsible AI policies.
- **Compliance & Audit:** Discover how to automate compliance monitoring, enhance your audit processes, and effectively manage AI risks from third parties.
- **Leadership & Strategy:** Master executive communication, drive essential organizational change, and craft future-proof AI security strategies.

Snap shots of the Participants of AI for Information Security Governance & Risk ManagementProfessionals" held on 02.08.25



5. **Topic : "Red Teaming from the Compliance Perspective"**
   Speakers : Mr. Yogesh Kale
   Date : 23-Aug-2025 (Saturday) Time : 5:30 PM - 7:30 PM IST
   Venue : Web-based ONLINE Session via Zoom Webinar Platform
   Free Attendance : 2 CPE Credits offered

Session Overview:

This session will provide practical demonstrations and a real-world case study to help you understand how Red Teaming can:

- **Validate Security Controls:** Assess the effectiveness of security controls and incident response capabilities.
- **Strengthen Risk Management:** Identify and address vulnerabilities that traditional audits might miss.
- **Translate Findings into Compliance:** Learn to convert technical findings into actionable audit evidence and risk registers.
- **Differentiate from Traditional Audits:** Discover how Red Teaming simulates real-world attacks to provide measurable insights beyond simple checklist assessments.

About the Speaker : Mr. Yogesh Kale

MR. YOGESH KALE, Manager of Security Consulting & Advisory at Gravity Innovision Solutions LLP. With over four years of experience in cybersecurity, he has a proven track record of providing security solutions and consulting to a wide range of organizations, helping them achieve and maintain compliance with frameworks like PCI DSS, ISO 27001, and GDPR.

This session is a must-attend for security practitioners, compliance officers, and IT auditors who wish to gain a strategic perspective on leveraging Red Teaming for operational resilience and compliance verification.

CPE Workshops:

1. **Topic : "The Chief Artificial Intelligence Officer (CAIO) Certification Program**
   Speakers : Mr. Kersi Porbunderwaa, Mr. Atul Juvle & Mr. Herman Huwyer
   Date : 29-Aug-2025 (Friday) to 31-Aug-2025 (Sunday) Time : 9:30 AM - 5:30 PM IST
   Venue : Web-based ONLINE Session via Zoom Webinar Platform / Physical Session at Chapter Office
   Free Attendance : 7 CPE Credits offered

The ISACA Bangalore Chapter is proud to support the **Certified Chief Artificial Intelligence Officer (CAIO) Certification Program**, delivered by the esteemed **Copenhagen Compliance**, from **August 29th to 31st, 2025**.

In a world increasingly driven by AI, mastering its governance, risk, and compliance is not just an advantage-it's a necessity. This program is designed to equip you with the knowledge and credentials to confidently lead the AI revolution and become a key player in shaping resilient AI ecosystems.

Here's what you can expect from this program:

- **Cutting-Edge Knowledge:** Dive deep into AI Governance, Risk & Compliance.
- **Practical Expertise:** Learn to implement the EU AI Act's Code of Practice and other global AI mandates.
- **Exclusive Networking:** Connect and collaborate with global AI governance experts.
- **Internationally Recognized Credential:** Future-proof your career with the prestigious CAIO certification.

The program will be delivered in a hybrid mode, allowing you to join us either in-person at the ISACA Bangalore Chapter Office or online via Zoom.

2. Topic : "How Secure Are We? Live Hacking Service"
Speaker : Mr. Vadivelan Sankar
Date : 20-Sep-2025 (Saturday) Time : 10:00 AM - 4:00 PM IST
Venue : ISACA Bangalore Chapter Office, Solus Jain Heights, Unit B10, 10th Floor, JC Road, Bengaluru.
Free Attendance : 7 CPE Credits offered

About the Session:

In today's threat landscape, knowing your security posture is non-negotiable. This live ethical hacking demo will showcase real-time cyberattacks, exposing vulnerabilities that are misunderstood and often go unnoticed. Learn from simulated intrusions how attackers exploit weak points - and how you can stop them.

Key Takeaways:

- Identify hidden cyber risks
- Understand real-world attack methods
- Learn mitigation strategies
- Be cybersecurity aware & promote a culture of digital resilience

About the Speaker : Mr. Vadivelan Sankar

MR. VADIVELAN SANKAR, CTO - Cyberium Labs. A seasoned red team expert and former Indian Navy cybersecurity auditor, Mr. Sankar brings over 26 years of experience across defense, consulting, and corporate cyber risk domains.

3. Topic : "Advancements in Space Technology - C5 and National Security"
Speakers : Various Speakers
Date : 27-Sep-2025 (Saturday) Time : 2:00 PM - 5:00 PM IST
Venue : Web-based ONLINE Session via Zoom Webinar Platform
Free Attendance : 3 CPE Credits offered

4. 28th Annual Karnataka Conference held on 8th & 9th August 2025 at Taj Hotel, Bengaluru

Theme : "Resilience by Design : Embedding Security, Audit & Governance in AI Driven Ecosystems"
Speakers : Various Speakers
Date : 08-Aug-2025 (Friday) & 09-Aug-2025 (Saturday) Time : 9:00 AM - 5:00 PM IST
Venue : The Taj Hotel, MG Road, Bengaluru
Free Attendance : 14 CPE Credits offered

Agenda Details

8th August 2025

08:30 - 09:30	**Registration**
09:30 - 09:40	**Welcoming the Special Chief Guest & Chief Guest to the venue**
09:40 - 09:45	**Welcome by Conference Chair** Mr. Deepak
09:45 - 10:00	**Special Chief Guest, Chief Guest & ISACA Office Bearers ascend the Dias** Dr. E. Khalieraaj, Director- NCSRC and Mr. Daljeet Kumar, IAS Dy Secretary of the Department of IT, BT, & Skill Development, Government of Karnataka
10:00 - 10:10	**Inauguration - Lighting the lamp**
10:10 - 10:15	**Welcome address by Chapter President** Ms. Vijayavanitha
10:15 - 10: 45	**Inauguration address by Special Chief Guest** Dr. E Khalieraaj, Director - National Cyber Security Research Council, New Delhi
10:45 - 11:15	**Keynote Address by Chief Guest** Mr. Daljeet Kumar, IAS- Dy Secretary of the Department of IT, BT, & Skill Development, Government of Karnataka
11:15 - 11:20	**Release the Conference Edition of Newsletter** Special Chief Guest & Chief Guest
11:20 - 11:30	**Felicitation** of exam toppers and white paper winners by Special Chief Guest & Chief Guest
11:30 - 11:45	**Exhibits & Tea Break**
11:45 - 12:20	**Keynote Address**: *Implementing secure digital transformation in the contracting space - NeSL Digital Document Execution (DDE) journey.* Ms. E P Nivedita IAAS, Executive Director (ED) & Chief Risk Officer (CRO) at NeSL (National E-Governance Services Limited)
12:20 - 13:00	**Keynote Address**: *Reimagining the Future Cyber Security Organization* Ms. Deepa Seshadri, Partner - Deloitte
13:00 - 14:00	**Lunch Break**
14:00 - 14:30	**Speaker Session**: *Auditing AI: Practical Approaches for Assurance in Machine Learning Models* Mr Kallol Kumar, Senior Director, Protiviti Member Firm for India
14:30 - 15:00	**Speaker Session**: *From Zero Trust to AI Trust: Evolving Cybersecurity for Autonomous Systems* Mr. Prabhu K, Vice President - Security & Engineering-SQ1
15:00 - 15:30	**Speaker Session**: *Humanising AI: How to Avoid the Mistakes of Inhuman IT Service Management* Ms. Katrina Macdermid, Co-founder & Director - HIT Global & Creator: Humanising IT
15.30 - 15.45	**Exhibits & Tea Break**
15.45 - 16:45	**Panel Discussion**: *Architecting for Adversity: Designing Robust AI Systems Against Malicious Attacks and Data Poisoning* Moderator: Mr. Gomeet Pant, Vice-President - Global Department Manager - Infosec Services, ABB Panelists: Mr. Devinder Singh, Cyber Security Leader-Carrier Ms. Sujatha Yakasiri, Sr. Application Security Architect at Farfetch, Portugal Mr. Rohan Kanungo, Google Cloud Office of the CISO Mr. Chandrasekar Rathinam, leadership role at SQ1 Security
16:50 - 17:20	**Keynote Speaker**: *The Battle for Digital Supremacy: AI in the Era of Ransomware* Mr. Sukrit Ghosh Director, DSCI | Data Security Council of India (DSCI)
17:20 - 17:50	**Speaker Session**: *Humanware - An Unencrypted Emotion - Cybersecurity X Storytelling* Ms. Sharada & Mr. Kamalakannan Durairaju & Partner
17:50 - 18:00	**Winners of Quiz & Thank You**

28th Annual Karnataka Conference

ISACA Bangalore Chapter

Resilience by Design: Embedding Security, Audit & Governance in AI - Driven Ecosystems.

9th August 2025

09:00 - 09:05	**Special Chief Guest, Chief Guest & ISACA office bearers ascend the Dais.** Welcome by ISACA Bangalore Chapter - President
09:05 - 09:10	**Felicitation** of Alliance University Mentors - by Special Chief Guest **Felicitation** of Quiz Winners - by Chief Guest
09:10 - 09:40	**Special Chief Guest Address** Dr. M.A. Saleem, DG & IGP Karnataka, Karnataka State Police
09:40 - 10:10	**Chief Guest Keynote Address**: AI-Powered Threat Intelligence and Proactive Defense Mr. Vadivelan Sankar, Co-Founder and CEO - Cyberium Labs Private Limited
10:10 - 10:45	**Keynote Address:** *Fortifying the Future: AI as Cyber Shield and Cyber Target* Mr. Akshay Garkel, Partner & Leader, Cyber at Grant Thornton Bharat
10:45 - 11:15	**Keynote Address**: Ensuring Data Privacy Compliance in AI Deployments Shri Vigneshwaran K, IAAS - Senior Deputy Accountant General, Karnataka, Bengaluru.
11:15 - 11:30	**Exhibits & Tea Break**
11:30 - 12:00	**Keynote Address**: *Resilience by Design: Embedding Security, Audit & Governance in AI-Driven Ecosystems* Lt Commander Mr. Amit Pal Singh, DGM – Cybersecurity, Siemens Healthineers
12:00 - 12:30	**Keynote Address**: *The distance between Zero Day Vulnerability and Zero Day Intelligence - Do we know the Unknown-Unknown?* Mr. Philip Varughese, President & Global Head – Strategic Growth at Cyfirma
12:30 - 13:00	**Speaker Session**: *Future-Proofing GRC: Anticipating Regulatory Evolution and Emerging AI Risks* Ms. Parimala Murthy - CISO Policy, Risk and IT control Framework Leader
13:00 - 14:00	**Lunch Break**
14:00 - 14:15	**Quiz by ISACA BC**
14.15 - 15:15	**Panel Discussion**: *Navigating the Regulatory Landscape: Future-Proofing AI-Driven Ecosystems for Evolving Compliance and Ethical Demands* Moderator: Mr. Babu Subramaniam Karunakaran, Head - IS Audit at Societe Generale Panelists: Mr. Chetan Anand, Digital Trust Leader and National Cybersecurity Scholar Mr. Rushabh Pinesh Mehta, GRC and Data Privacy Leader Mr. Sangeeth Keeriyadath, AI Solution Architect- State Street Corporation
15:15 - 15:30	**Exhibits & Tea Break**
15:30 - 15:40	**Winners of Quiz** Passport Lucky Draw
15:40 - 15:50	**Valedictory Address** Mr. Raghu R V, ISACA Regional Ambassador
15:50 - 16:00	**Vote of Thanks** Ms. Suma, Secretary - ISACA BC

SPONSOR

GOLD: SQ1 nextgen cybersecurity

SILVER: protiviti Global Business Consulting

CYBER PARTNER: tsaaro consulting

Get ahead in your career

Sign up for ISACA membership today!
chapter@isacabangalore.org | +91 98865 08515

THREAT HUNTING OUTSTRIPS THREAT INTELLIGENCE TO RUPTURE CYBERCRIME TERRAIN

By : Ragini Sinha

ABOUT WRITER : RAGINI SINHA, E mail ID: sinha.ragini@gmail.com

Profession : International freelance creative Writer

Academic education : PG in Psychology.

Writing expertise : To introduce, writer is a passionate international creative writer. Her writing career has long voyage and great fit for delivering premium articles and research documents. She has an expertise in test development in reasoning and aptitude, social sciences, management, and Information technology of various examination bodies.

Technical Knowhow: Former guest member of various leading examination bodies.

COMPARATIVE SCRUTINY OF THREAT HUNTING AND INTELLIGENCE:

Cybersecurity is an omnipresent phenomenon in the digital business world. Myriads of defensive techniques are embraced by leading corporations to evade severe cyber threats to computer systems, networks, and critical infrastructure from hackers. Threat hunting is the emergent cyber security defender that combat and shield a workplace's digital infrastructure from unwanted breaches. In threat hunting practice, cyber experts vigorously look for and detect cyber risk factors that have been slipped and are invisible in the digital system of a company. Threat hunting is conducted with a range of manual and automated techniques to spot and alleviate malicious activities and cyber threats at inception stage to avoid any significant damage to corporations. On the other hand, threat intelligence techniques are implemented in the cyber ecosystem to arrest constant cyber threats bombarded by hackers. Core function of threat intelligence in cybersecurity is to detect the activities of threat players, their tactics, and probable weaknesses in the system to provide a strong defensive layer around the digital system and react to any proactively strengthened defenses and respond to cyber-attacks in a timely manner.

Cyber hunting is meticulously involved in dissecting the cyber undetected threats in computer networks through blending digital forensics and incident response tactics that can derail the business functions and other sensitive processes. Software companies are soft targets of cyber fraudsters for data robbery or disrupting the network. Threat hunting practices are smart tactics to expose advanced persistent threats that silently present in the system and remain unnoticed. Cyber hunters tactfully distinguish unusual behavior patterns that pose insider threats in companies.

Threat hunting process involves various steps to alert the system from cyber threats. Threat hunting tactics proactively checks system's memory for malicious activity using memory junkyards, which are snapshots of a random-access memory (RAM) in a device at a specific point in time. Threat hunting process thoroughly investigates server images to identify any threat bustle and scrutinizes endpoint protection data to detect suspicious behaviors of cyber attackers.

THREAT HUNTING OVERRIDES THREAT INTELLIGENCE IN CYBER THREAT ECOSYSTEM:

Gauging the cyber detecting capabilities of both cyber threat hunting and threat intelligence, threat hunting thoroughly searches the pattern of cyber threats at an early stage of security incidents and prevents from wrecking the network that may cause severe fiscal damage to the company. Profound scrutiny of insider threats

that are undetected enable cyber professionals to devise remedial plans to exterminate threats. Whereas, threat intelligence collates massive information about probable or prevailing cyber threats to inform companies to protect from attackers. Cyber experts of threat hunting dynamically tap and counteract cyber threats within the network.

VISIBLE IMPACT OF THREAT HUNTING AND THREAT INTELLIGENCE ON CYBER SYSTEM:

Though both threat hunting and threat intelligence are robust practices to spot cyber threats, these differently impact the cyber system on the company. Threat intelligence is about amassing, evaluating, and spreading vast information about all possible cyber threats. It equips companies to know about threat actors, their bad intentions, malicious strategies, and procedures. Threat intelligence tactics inform about the nature of cyber threats, anticipate types of cyber-attacks and defensive tactics to companies. Threat hunting overpowers threat intelligence in the situations where traditional, automated security systems might fail to locate cyber threats silently embedded in the system to crush cruel intentions of fraudsters.

FINAL APPRAISAL:

Threat hunting bolsters the security layer of multinational companies struggling to deal with cyber attackers. The crucial role of threat hunting is to expose the inherent cyber threats and offer mitigating tactics to prevent colossal damage. Putting a light on threat intelligence, it is a smart tactic to gather, analyze and provide relevant data about the current and evolving threats network to create a defensive ecosystem. Cyber hunting practices penetrate in networks to detect suspicious behavior and silent threats that may ruin the digital landscape. Threat hunting proves to be more effective to offer security and provide defensive measures to evade from threat actors or respond quickly to combat cyberthreats and tendencies.

Important note: Above technical article is based on resourceful environmental inputs and solely the self-analysis of the writer. This technical writing is for general awareness and is not intended for technical implementation. Any resemblance is just a coincidence. Writer is not responsible for any disagreement.

Operationalizing AI Accountability : A Multi-Layered Approach to Governance, Risk Management & Compliance

By : Mandara Mulgund

ABSTRACT : As AI systems evolve from narrowly scoped tools to enterprise-critical infrastructure, the need for comprehensive, end-to-end accountability becomes a complex, multidisciplinary engineering imperative. This whitepaper presents a robust, multi-layered architecture designed to operationalize AI accountability throughout the entire model lifecycle. The approach integrates secure MLOps pipelines, automated compliance workflows, and systemic governance mechanisms to ensure transparency and trust. Aligned with leading global standards-such as ISO/IEC 42001, the NIST AI Risk Management Framework, and the EU AI Act-the framework provides actionable mechanisms for enforcing policies at design time, enabling observability at runtime, and ensuring auditability post-deployment. It includes technical strategies like policy-as-code, cryptographic model signing, explainability through SHAP and LIME, drift-aware retraining, and federated audit networks. Real-world case studies from sectors like healthcare and e-commerce demonstrate how these controls enhance fairness, regulatory compliance, and stakeholder trust. Ultimately, the architecture embeds accountability at every layer, supporting scalable, trustworthy, and transparent AI development.

Keywords for Whitepaper Distribution

- AI Accountability
- Enterprise AI Governance
- Responsible AI Architecture
- ISO/IEC 42001
- NIST AI RMF
- EU AI Act Compliance
- MLOps and Policy-as-Code
- AI Lifecycle Risk Management
- Explainable AI (XAI)
- AI Auditability
- Drift Monitoring
- Federated Learning & Auditing
- Regulatory Technology (RegTech)
- Secure AI Deployment
- Data Privacy in AI
- Human-in-the-Loop AI
- AI Transparency Standards
- Model Risk Classification
- Compliance Automation
- Ethical AI Engineering

Introduction:

Artificial Intelligence (AI) has moved beyond experimental deployments to become a core layer of decision automation in financial services, healthcare, law enforcement, and infrastructure. These systems, often based on black-box deep learning models, pose significant risks: epistemic uncertainty, adversarial vulnerability, data drift, and ethical opacity. Traditional IT General Controls (ITGC) and Software Development Lifecycle (SDLC) methods are inadequate for managing AI's probabilistic nature and self-modifying behavior.

Operationalizing accountability requires a techno-legal framework integrating computational explainability, cryptographic integrity, runtime assurance, and policy traceability. This white paper deconstructs the AI lifecycle

into auditable, enforceable control zones and proposes an architecture for embedding accountability at every stage - from model conception to deprecation.

1. Architectural Foundations for Accountable AI

An accountable AI architecture is defined by five core principles:

A. Systemic Observability: Full-stack monitoring across training, inference, and feedback.
Telemetry is embedded throughout the pipeline to track model behavior, detect drift, and enable real-time diagnostics.

B. Policy Binding: Business and legal rules enforced via policy-as-code.
Executable constraints ensure compliance and prevent unauthorized actions across data handling and model deployment.

C. Explainability by Design: Built-in model introspection at every layer.
Explainability tools (e.g., SHAP, LIME) are integrated into the workflow, enabling transparency for developers, auditors, and users.

D. Trust Anchors: Security rooted in hardware-backed attestation and cryptographic integrity.
Techniques like secure enclaves and signed artifacts ensure tamper resistance and verifiable trust.

E. Lifecycle Governance: Centralized tracking of models, data, and audit events.
Registries log all key artifacts and metrics-supporting traceability, accountability, and ongoing compliance.

1.1. System Layering The architecture decomposes into five layers:

A. Data Layer: Data lakes, metadata catalogs, and version control.
Foundation for reliable ML begins with scalable storage, structured metadata, and reproducible datasets using tools like Delta Lake, Data Catalogs, and DVC.

B. Feature Layer: Feature stores, lineage tracking, and transformation logs.
Centralized feature management ensures consistency across training and inference, with lineage graphs capturing data provenance and transformation steps.

C. Model Layer: Versioned models with full training context.
Model registries track versions, training metadata, and hyperparameters-enabling reproducibility, comparison, and rollback.

D Serving Layer: Scalable, containerized inference with deployment controls.
Models are deployed via microservices with support for A/B tests, canary releases, and shadow modes to reduce risk.

E. Monitoring Layer: Real-time drift, fairness, and explainability checks.
Continuous monitoring surfaces bias, performance degradation, and opaque behavior through integrated audit and alerting tools.

2. Technical Controls Across the AI Lifecycle

2.1. Data Ingestion and Curation

A. Lineage Tracking: Column-level data provenance via Apache Atlas or OpenLineage. Lineage tools trace how data flows and transforms across systems, enabling auditability, reproducibility, and impact analysis for every attribute used in modeling.

B. Anonymization Pipelines: k-anonymity and t-closeness applied during preprocessing.
Privacy-preserving algorithms are embedded early in the data pipeline to protect sensitive attributes while retaining analytical utility, ensuring regulatory compliance (e.g., GDPR, HIPAA).

C. Bias Surface Mapping: PCA and t-SNE visualize demographic patterns and imbalance.
Dimensionality reduction techniques reveal clustering and representation gaps across protected groups, supporting early detection of bias in training datasets.

2.2. Feature Engineering

A. Immutable Feature Logging: Each derived feature is traceably linked to raw data via UUIDs.
This ensures full provenance and auditability, allowing reconstruction of feature generation pipelines and verifying data integrity.

B. Adversarial Feature Testing: Inject noise to assess model robustness against perturbations.
Simulated adversarial inputs test feature stability and reveal vulnerabilities to input manipulation or data drift.

C. Correlation Sanitization: Eliminate proxy variables using mutual information thresholds.
Features highly correlated with sensitive attributes are identified and removed to mitigate indirect bias and ensure fairness.

2.3. Model Development

A. Model Cards v2: Standardized templates capturing design assumptions, training details, and validation schemas.
These enforced templates provide transparent documentation for stakeholders, improving model understanding and trustworthiness.

B. Risk Tags: Models labeled with risk scores reflecting criticality, complexity, and explainability.
Risk tagging guides governance policies, triggering additional controls for high-risk models.

C. Differential Privacy in SGD: e-differential privacy integrated into training via TensorFlow Privacy.
Privacy-preserving stochastic gradient descent protects sensitive training data by adding controlled noise, ensuring compliance with data protection laws.

2.4. Model Evaluation

A. Multi-Angle Testing: Evaluate model performance across intersectional demographics and stress scenarios.
Testing ensures equitable outcomes by assessing behavior on diverse groups and under varied data perturbations.

B. Counterfactual Sensitivity Analysis: Identify minimal input changes that cause prediction shifts.
This analysis reveals model decision boundaries and vulnerabilities, supporting explainability and robustness.

C. Fairness Certification: Apply fairness metrics like Equal Opportunity and Predictive Parity before deployment.
Models must meet defined fairness thresholds to pass certification, reducing bias risks in production.

2.5. Deployment and Serving

A. Immutable Inference Logs: Store every prediction with input, output, and feature attribution vectors for full traceability.

B. Inference Signatures: Generate and store SHA-256 digests per model version on append-only logs to ensure integrity.

C. Runtime Feature Encryption: Homomorphic encryption for sensitive inputs in medical/financial use cases.

2.6. Monitoring and Feedback

A. Online Drift Detection: Use Kolmogorov-Smirnov and Jensen-Shannon divergence tests to detect data shifts in real time.

B. Explainer APIs: Provide SHAP, LIME, and Integrated Gradients as REST endpoints to support auditability and transparency.

C. Drift-Aware Retraining: Automate retraining pipelines triggered by model health metrics to maintain performance.

3. AI Governance Structures

3.1. Governance Frameworks

A. ISO/IEC 42001 Alignment: AI policies are mapped to system-level controls with clear auditability objectives.

Governance frameworks align with ISO/IEC 42001 by translating high-level AI principles-such as fairness, transparency, and accountability-into enforceable system controls. Each control is tied to measurable outcomes and logging requirements, enabling traceable compliance across the ML lifecycle and facilitating third-party audits.

B. Three Lines of Defense: Governance roles are embedded across development, compliance, and audit functions.

Responsibility for AI risk is distributed using the Three Lines of Defense model:

- 1st line: Model developers apply policies and conduct testing.
- 2nd line: Compliance teams validate adherence to standards and assess risk posture.
- 3rd line: Internal audit independently reviews systems, controls, and records for assurance.

This structure ensures layered oversight and accountability.

C. Model Risk Classification Matrix: Models are scored along business impact, explainability, and autonomy dimensions.

A standardized risk matrix is used to assess each model's potential risk. Criteria include the model's decision criticality, level of human oversight, and interpretability. The resulting classification guides governance requirements, such as mandatory reviews, documentation depth, or deployment restrictions.

3.2. Control Implementations

A. MLOps with Control Gates: Control points embedded in CI/CD pipelines for model sign-off, compliance checks, and security scans.

Automated control gates are integrated into MLOps workflows to enforce policy adherence at critical stages-such as model validation, approval, and deployment. These include checks for model performance thresholds, compliance attestations, license validation, and vulnerability scans. Models failing any gate are blocked from progressing to production, ensuring only verified artifacts are deployed.

B. Access Governance: Role-based model access enforced via Open Policy Agent (OPA).

Access to models and ML artifacts is tightly controlled using role-based access controls (RBAC) defined and enforced through OPA policies. Permissions are scoped to roles (e.g., data scientist, reviewer, auditor) and applied consistently across environments. This minimizes unauthorized access, supports separation of duties, and enables dynamic policy updates without redeploying infrastructure.

C. Audit-Ready Registries: All artifacts-models, logs, and metrics-are hashed and stored with forensic integrity. Model registries and associated artifact stores maintain tamper-evident records by hashing and versioning all components (e.g., model binaries, training logs, evaluation metrics). These immutable logs support retrospective analysis, legal defensibility, and regulatory audits, forming a provable chain of custody for every model lifecycle event.

4. Regulatory Alignment and Compliance Enforcement

4.1. EU AI Act Controls

A. Risk Tier Mapping: Model risk levels are defined at design time and enforced via policy-as-code. Models are classified into risk tiers (e.g., low, medium, high) based on use case sensitivity, regulatory exposure, and business impact. These tiers dictate required controls-such as explainability, approval gates, or audit trails-enforced automatically through policy-as-code tools like OPA. This ensures consistent governance across the ML lifecycle.

B. Conformity Assessment Workflows: Compliance documentation is auto-generated and stored in the model registry. Upon registration, models trigger workflows that compile key compliance artifacts-data lineage, metrics, validation reports-into structured documentation. This is versioned and attached to each model entry in the registry (e.g., MLflow), streamlining audit readiness and regulatory alignment.

C. Logging Mandates: Operational telemetry is streamed in real time to immutable log sinks. Inference logs, model outputs, and system metrics are captured via observability tools (e.g., Kafka, Fluentd) and stored in append-only object stores. These immutable logs support traceability, incident response, and compliance verification in production environments.

4.2. GDPR and Data Rights

A. Right to Explanation: Enabled through human-in-the-loop workflows with visual attribution summaries. To meet legal and ethical obligations around explainability (e.g., GDPR Article 22), model predictions are accompanied by intuitive visualizations-such as feature attributions or saliency maps. When required, human reviewers can validate or annotate these outputs, forming part of a traceable review workflow that ensures decisions are understandable and accountable.

B. Automated Decision Notices: Generated by decision tracking services that record human overrides. All automated decisions are logged with metadata, including model confidence, input features, and decision rationale. If a human overrides a model's decision, that action is recorded alongside the original output. This creates a transparent audit trail and supports compliance with requirements for individual notice and review.

C. Data Subject Traceability: End-to-end lineage is maintained from source data to final inference per datapoint.
Every prediction is linked back to its originating data inputs, transformation steps, and model version. This source-to-inference trace enables organizations to respond to data subject requests (e.g., access, rectification, erasure) and supports robust auditability and debugging in high-stakes environments.

5. Advanced Techniques for Explainability and Fairness

5.1. Causal Explainability

A. Structural Causal Models (SCM): Defines explicit DAGs to understand mediating vs confounding variables.

B. Do-Calculus Audits: Evaluates fairness under interventions rather than observed correlations.

5.2. Robust Fairness Engineering

A. Ensemble Fairness: Blending models optimized on different fairness metrics.

B. Adversarial Debiasing: Use of gradient reversal layers to minimize attribute leakage.

C. Conformal Prediction Bounds: Provides calibrated uncertainty scores per prediction.

6. Case Studies

6.1. Healthcare: Radiology Diagnostics Platform

A leading hospital network deployed a convolutional neural network (CNN)–based image classification pipeline for automated chest X-ray analysis targeting pneumonia and pulmonary embolism detection. Despite strong overall accuracy, post-deployment evaluation exposed a disproportionate rate of false negatives among underrepresented demographic groups, particularly elderly and minority patients. This raised concerns about model fairness, clinical safety, and regulatory compliance.

A. Mitigations Implemented:

- Federated Learning: The network adopted federated learning frameworks (e.g., TensorFlow Federated) to train models across multiple hospital sites without centralizing sensitive patient data, preserving privacy and adhering to HIPAA standards. This approach enabled the incorporation of diverse, geographically distributed datasets, improving model generalizability.
- Bias Audits: Comprehensive fairness evaluations utilized statistical parity metrics, including Equal Opportunity Difference and Demographic Parity Difference, stratified by patient race, age, and gender cohorts. These audits identified specific subpopulations where performance gaps persisted.
- Data Rebalancing: Synthetic oversampling techniques (e.g., SMOTE) were employed to augment rare pathology-demographic combinations, mitigating class imbalance and enhancing feature representation for minority groups.
- Governance Update: Radiologists were integrated into a human-in-the-loop (HITL) workflow that mandated manual review for all model predictions with confidence scores below a defined threshold, ensuring clinical oversight and reducing diagnostic errors.

B. Outcome:

- The enhanced pipeline yielded a 21% increase in recall rates for underrepresented demographic segments, significantly reducing missed diagnoses.
- The system achieved compliance with HIPAA regulations and the FDA's Good Machine Learning Practices (GMLP), ensuring robust data privacy and quality management.
- Additionally, SHAP-based local explainability modules were embedded directly within the radiologists' diagnostic interface, providing interpretable feature attributions that facilitated clinical trust and decision validation.

This multi-faceted approach demonstrates how combining advanced technical solutions with clinical governance can address fairness and safety challenges in AI-powered healthcare applications.

6.2. E-Commerce: Product Recommendation Engine

A global e-commerce platform deployed a graph neural network (GNN) to personalize product recommendations based on user browsing, purchase, and engagement signals. Post-deployment analysis revealed systemic biases favoring dominant brands and reinforcing filter bubbles, limiting product diversity and consumer choice.

A. Mitigations Implemented:

- Fairness-Aware Ranking: Introduced a multi-objective ranking function that balances relevance, novelty, and exposure parity across vendors and product categories.
- Explainable Recommendations: Integrated feature attribution methods (e.g., GNNExplainer) to highlight the rationale behind each recommendation, improving algorithmic transparency.
- Drift Monitoring: Established real-time monitors for both demographic usage drift and concept drift in user behavior, triggering retraining of the model when significant deviation was detected.
- Transparency Dashboard: Deployed a consumer-facing interface allowing users to view, adjust, and opt out of influence signals driving personalized recommendations.

B. Outcome:

- Brand diversity in top-10 recommendations increased by 36%.
- Improved consumer trust and engagement through actionable transparency tools and feedback loops.
- Achieved compliance with regional consumer protection regulations, algorithmic transparency mandates, and emerging digital service acts.

7. Future Directions: Towards Autonomous Accountability

7.1. Autonomous Governance

A. AI-in-the-Loop Auditing: Leverage large language models (LLMs) to automatically analyze model logs and flag anomalies for faster, intelligent oversight.

B. Self-Documenting Pipelines: Automate creation of traceability graphs, data cards, and audit narratives to maintain continuous and up-to-date compliance records.

7.2. Assurance as Code

A. Control Templates: Use GitOps-driven YAML templates to embed regulatory checkpoints directly into deployment pipelines, ensuring consistent compliance enforcement.

B. Blockchain Anchoring: Anchor cryptographic hashes of logs, models, and controls on public blockchains to enable immutable, third-party verifiability.

7.3. Cross-Enterprise Assurance Fabric

A. Federated Audit Networks: Implement shared assurance protocols across vendors using zero-knowledge proofs to preserve privacy while enabling joint audits.

B. Decentralized Identity (DID): Assign verified identities to developers and auditors for accountability and traceability of model changes.

8. Conclusion

Operationalizing AI accountability is not a checklist-it is an architectural doctrine. This paper proposes a comprehensive technical blueprint that spans design-time controls, runtime observability, post-hoc auditability, and regulatory harmonization. By integrating rigorous MLOps, explainability tooling, and automated assurance workflows, organizations can transform opaque, stochastic systems into verifiable, trustworthy AI assets. As AI proliferates across high-stakes domains, accountability must be encoded-not inferred.

9. References

- *Doshi-Velez, F., & Kim, B. (2017): Towards A Rigorous Science of Interpretable Machine Learning. arXiv:1702.08608*
- *European Commission. (2024): The EU Artificial Intelligence Act.*
- *NIST (2023): Artificial Intelligence Risk Management Framework.*
- *ISO/IEC 42001:2023: Artificial Intelligence Management System Standard.*
- *OECD. (2019): OECD Principles on Artificial Intelligence.*

28TH ANNUAL KARNATAKA CONFERENCE
HELD ON 8th & 9th AUGUST 2025 AT TAJ HOTEL, BENGALURU.

The Annual Karnataka Conference 2025, held at the Taj MG Road, Bangalore, on August 8th and 9th, 2025, was an enriching and notable success. Theme: The conference theme was "Resilience by Design: Embedding Security, Audit & Governance in AI-Driven Ecosystems." Content: The event featured a diverse lineup of speakers from various industries who shared critical insights on current trends, challenges, and best practices in information security, risk management, and governance. Attendance & CPE: The conference attracted approximately 450+ attendees. These sessions provided an excellent opportunity to earn valuable CPE credits, totaling 6,412 hours, which represents a 31% increase compared to AKC 2024. Special Incentive: Early bird registrants were provided a complimentary online training workshop titled "AI for Information Security Governance & Risk Management Professionals."


Annual
Karnataka Conference
ISACA Bangalore Chapter
ISACA
Bangalore Chapter
Resilience by Design: Embedding Security,
Audit & Governance in AI-Driven Ecosystems.


Annual
Karnataka Conference
ISACA Bangalore Chapter
ISACA
Bangalore Chapter
Resilience by Design: Embedding Security


dive
Labs


Annual
Karnataka Conference
ISACA Bangalore Chapter
ISACA
Bangalore Chapter
Resilience by Design: Embedding Security,


Quiz Winners


Valedictory Address
R V Raghu
ISACA Global Ambassador,
ISACA
Annual
protiviti

ALL-INDIA PRESIDENTS' MEET WITH MR. ERIC PRUSCH, CEO OF ISACA GLOBAL
HELD ON AUGUST 23rd 2025 AT THE BANGALORE CHAPTER OFFICE, BENGALURU

CAIO (CHIEF ARTIFICIAL INTELLIGENCE OFFICE) CERTIFICATION PROGRAM

CONDUCTED FROM AUGUST 29th - 31st 2025 AT THE BANGALORE CHAPTER OFFICE, BENGALURU IN A HYBRID FORMAT (IN-PERSON AND ONLINE VIA ZOOM)

ADVANCING ACADEMIC OUTREACH
HELD ON 10th SEPTEMBER 2025 AT PRESIDENCY UNIVERSITY, BENGALURU.

ISACA Student Group Launched at Presidency University The ISACA Bangalore Chapter achieved a major milestone in its academic relations by officially inaugurating a new ISACA Student Group (ISG) at Presidency University, Bengaluru, on September 10, 2025.

This launch solidifies our commitment to fostering the next generation of professionals in cybersecurity, audit, and IT governance. The inauguration was highly successful and attended by distinguished academic and chapter leadership.

Key university leaders present included Dr. Mahalaxmi (Associate Dean), Dr. Shakkeera L (Associate Dean), Dr. Robin Rohit Vincent (HOD), Dr. S.P. Anandaraj (Head, CSE), and Mr. Likhith (Assistant Professor). The ISACA Bangalore Chapter was proudly represented by Vijayavanitha S (President), Satish Kumar (CISO Fintech), and Sampathkumar Krishnasamy (Director, Academic Relations).

Further demonstrating our commitment to their success, the ISACA Bangalore Chapter conducted an Orientation Program for the newly formed Presidency University ISG core team on September 27, 2025, held at the Chapter Office. The new student leadership has already demonstrated commendable dedication and enthusiasm in their commitment to building a strong professional community.

We are confident this group will become a cornerstone for professional growth and learning at Presidency University and look forward to supporting these emerging leaders and their future endeavors.


ISACA STUDENT
GROUP
Inaugural Ceremony


School of Computer
d Engineering


with ISACA
Certification
Get certified and get ahead.

ACADEMIC RELATIONS : ISACA STUDENT GROUP
INAUGURATED ON 19th SEPTEMBER 2025 AT JAIN UNIVERSITY, BENGALURU.

The ISACA Bangalore Chapter marked a significant milestone in its academic outreach by officially inaugurating a new ISACA Student Group (ISG) at Jain University, Bengaluru, on September 19, 2025.

This development underscores our commitment to advancing IT Governance, Cybersecurity, and Audit by actively nurturing future-ready professionals within the region.

The landmark inauguration ceremony brought together prominent figures from both the industry and academia. The event was graced by Chief Guest Mr. Raghu Iyer, ISACA International Ambassador, alongside key academic leaders from Jain University, including Dr. Asha Rajiv and Dr. Reena Susan Philip. The ISACA Bangalore Chapter leadership was present to lend its crucial support. We eagerly anticipate the growth and success of the Jain University ISG and look forward to supporting their journey as they build a thriving professional community committed to the ISACA mission.

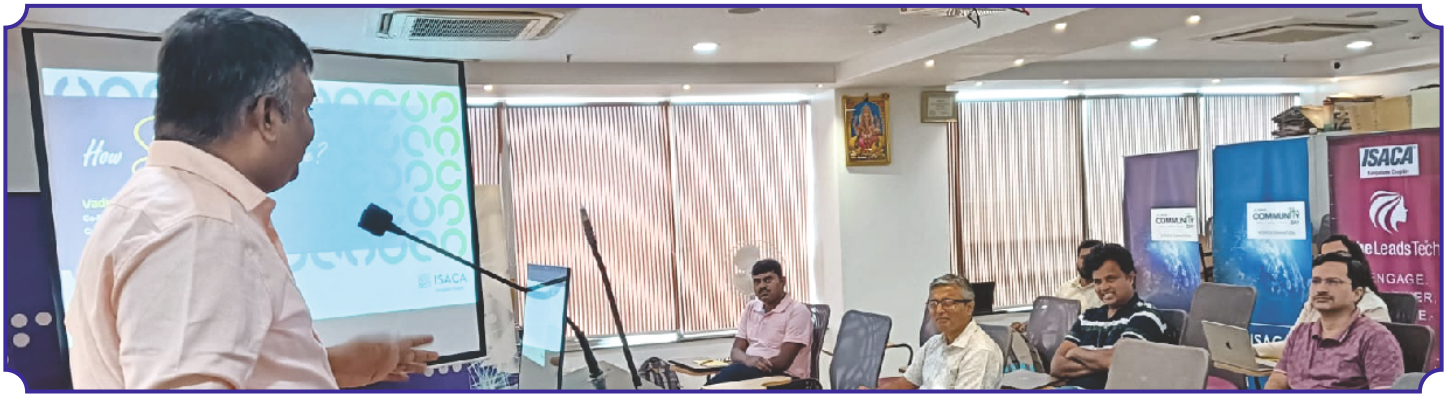

Move Your
Career Forward
with ISACA
Certification


Move Your
Career Forward
with ISACA
Certification
ISACA


Move Your
Career Forward
with ISACA
Certification


JAIN

"HOW SECURE ARE WE - LIVE HACKING SERVICE" EVENT
HELD ON 20th SEPTEMBER 2025 AT THE BANGALORE CHAPTER OFFICE, BENGALURU



ISACA STUDENT GROUP ON-BOARDING SESSION FOR PRESIDENCY STUDENTS
CONDUCTED ON 27th SEPTEMBER 2025 AT THE CHAPTER OFFICE, BENGALURU

ISACA COMMUNITY DAY
HELD ON 4th OCTOBER 2025 AT BANGALORE GO RAKSHANA SALA


ISACA


COMMUNITY DAY
COMMUNITY DAY


COMMUNITY DAY
COMMUNITY DAY

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

SQ1

nxtgen cybersecurity

AI-Enabled Cybersecurity & Compliance Solutions

www.sq1.security

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