



Emerging Technology Risks

From Digital Risk to Intelligent Assurance

Friday, November 20, 2026

8:00 a.m. – 4:30 p.m.

(8 CPE/CPD Credits)

Technology is no longer simply supporting the organization—it is increasingly making decisions, executing processes and reshaping how work gets done. As artificial intelligence, autonomous agents, cloud platforms, connected systems and advanced automation become embedded across the enterprise, they introduce significant opportunities alongside new operational, cybersecurity, privacy, regulatory and ethical risks.

For Internal Audit and Technology professionals, the challenge has moved beyond understanding individual technologies. We must evaluate how these technologies interact, how quickly risks can emerge and whether governance and controls can keep pace with innovation. Traditional, periodic auditing alone may no longer provide sufficient assurance in an environment where systems learn, decisions are automated and third-party technologies are deeply integrated into critical business processes.

This event will bring together practitioners who are working at the intersection of technology, risk and assurance. We will examine the evolving cyber threat landscape; the governance and responsible adoption of artificial intelligence; the risks created by AI agents, data dependencies and interconnected third parties; and the growing importance of operational and cyber resilience. We will also explore how leading organizations are modernizing Internal Audit through data analytics, continuous monitoring, intelligent automation and AI-enabled auditing.

Looking beyond 2026, Internal Audit has an opportunity to become more dynamic, technology-enabled and forward-looking—providing assurance not only over today's controls, but also over the organization's readiness for what comes next. Attendees will leave with practical insights into the emerging technologies and risks that deserve attention now, the questions audit leaders should be asking, and the capabilities their teams will need to remain relevant and effective in the years ahead.

Agenda

- **7:30 – 8:00 AM – REGISTRATION/LOG - IN**
- 8:00 – 8:05 AM – Opening Business Items
- 8:05– 9:00 AM – You Cannot Govern What You Cannot See: Data Discovery, AI Inventories and Shadow AI
- 9:00 – 10:00 AM – When AI Becomes an Actor: Human Behavior, Agentic Risk and Organizational Control
- **10:00 – 10:15 AM – BREAK**
- 10:15 – 11:00 AM – Auditing What Comes Next: AI, Cyber Risk and the Future of Assurance
- 11:00 – 12:00 PM – From Cyber Risk Assessments to Continuous Resilience
- **12:00 – 1:00 PM - LUNCH**
- 1:00 – 2:15 PM– AI in Action: Reimagining Internal Audit and Controls
- 2:15 – 3:15 PM – Closing the Cybersecurity Capability Gap: What Organizations and Internal Audit Keep Getting Wrong
- **3:15 – 3:30 PM – BREAK**
- 3:30 – 4:25 PM – Keeping Humans Accountable in an AI-Enabled Organization
- 4:25 – 4:30 PM – Wrap Up and Closing Comments

8:00 – 8:05 AM: Welcome and Opening Remarks

8:05 – 9:00 AM: You Cannot Govern What You Cannot See: Data Discovery, AI Inventories and Shadow AI

Gal Ringel | Co-Founder and Chief Strategy Officer, MineOS



Organizations cannot govern risks they cannot see. This session examines how sensitive data, unsanctioned AI tools, SaaS applications and third-party dependencies spread across the enterprise, and how continuous discovery, classification and evidence can help management and Internal Audit establish meaningful oversight.

Gal Ringel is Co-Founder and Chief Strategy Officer of MineOS, an enterprise AI governance and privacy platform. After serving as CEO for six and a half years, he continues to shape the company's strategy and approach to continuous data, privacy and AI governance. Before founding Mine, Gal served six years in the Israeli intelligence unit 8200 and spent four and a half years as a venture capital investor, deploying approximately \$50 million across more than 20 technology companies. His work focuses on helping organizations discover and govern sensitive data, shadow IT, AI systems and emerging agentic risks through continuous visibility, context and evidence.

9:00 – 10:00: When AI Becomes an Actor: Human Behavior, Agentic Risk and Organizational Control

Hanah-Marie Darley | Co-Founder and Chief AI Officer, Geordie AI



The session examines how organizations safely adopt increasingly autonomous systems, align agent behavior with human intent, establish meaningful oversight and prepare for technological and behavioral failures.

Hanah-Marie Darley is Co-Founder and Chief AI Officer of Geordie AI, where she helps organizations adopt agentic AI securely, responsibly and at scale. She brings more than a decade of experience spanning artificial intelligence, cybersecurity, threat intelligence, geopolitical analysis and applied psychology. Before co-founding Geordie, Hanah-Marie held leadership roles at Darktrace, including Director of Security and AI Strategy, Field CISO and Director of Threat Research. Her human-centered approach to AI governance focuses on understanding autonomous system behavior, aligning AI actions with human intent and enabling innovation without sacrificing security, transparency or oversight.

10:00 – 10:15: Break

10:15 – 11:00 AM: Auditing What Comes Next: AI, Cyber Risk and the Future of Assurance

Russell Safirstein | President & CEO, NexAI Cyber



As technology increasingly makes decisions and executes business processes, Internal Audit must rethink how it identifies risk and provides assurance. This session presents a practical framework for auditing AI, cybersecurity, automation and other emerging technologies while maintaining independence and focusing on the risks that matter most.

Russell Safirstein is President & CEO for NexAI Cyber, a human-led, technology-enabled cybersecurity and AI firm. He is a senior executive and a progressive thinker with over 30 years of experience and has been successful in bringing non-traditional solutions to an ever-changing work environment. Russell has co-founded several organizations that specialize in Cyber, AI & Machine Learning and holds several patents. Russell is a highly regarded and sought after speaker on cyber security, technology, audit and risk practices.

Russell started his career with KPMG in their Financial Institution practice after graduating from Adelphi University with a BBA in Accounting. He served over 15 years as a CAE (Chief Audit Executive) with several large public companies.

11:00 – 12:00 PM: From Cyber Risk Assessments to Continuous Resilience

Jack Thompson | Field CISO, Cynomi (former CISO, Indianapolis Colts)



Annual assessments and compliance checklists provide only a snapshot of cyber risk. This session examines how organizations can create continuous cybersecurity programs that connect risk identification, remediation, business continuity and executive reporting and what Internal Audit should examine to determine whether those programs are working.

Jack Thompson is Field CISO at Cynomi, where he helps organizations strengthen, scale and communicate the business value of their cybersecurity, risk and compliance programs. Previously, Jack served as Director of Information Security, Risk and Compliance for the Indianapolis Colts and led information security at Bastian Solutions. He also served for more than a decade across the U.S. Army and U.S. Air Force in military intelligence and cyber

operations. Drawing on experience across the public and private sectors, Jack is known for translating complex technical risks into practical business priorities and helping organizations build stronger security cultures and operational resilience.

12:00-1:00 PM – Lunch Break

1:00 – 2:15 PM: AI in Action: Reimagining Internal Audit and Controls

Jingwei “Mavis” Jiang, MBA, CFA | Senior Manager, Deloitte • Peter Baciorowski, CISA | Managing Director, Deloitte

AI is reshaping how internal audit and controls professionals approach their work, creating new opportunities to enhance efficiency, quality, and insights. This session moves beyond the hype to explore practical applications of AI across the risk and controls lifecycle, from risk assessment and planning to controls evaluation, testing, and reporting. Through real-world scenarios and a live demonstration of AI-enabled capabilities, attendees will see how technology can streamline manual processes, accelerate testing, and generate more meaningful insights. The session will highlight how combining human expertise with AI can help practitioners shift their focus toward higher-value activities and deliver more effective, forward-looking assurance.



Mavis Jiang, MBA, CFA, is a Senior Manager at Deloitte with over 15 years of experience in financial services. Since joining Deloitte's Audit Innovation group, she has been at the forefront of the firm's audit and assurance transformation and innovation journey. As the FSI Industry Lead for Audit Assurance Analytics, she leads the development and deployment of technology-enabled solutions that address evolving client needs, leveraging advanced analytics, automation, AI and other emerging technologies. Mavis also serves as Deloitte Transformation Coach, supporting strategic client pursuits by helping engagement teams demonstrate the value of AI, analytics, and technology-enabled transformation

in enhancing audit and assurance quality, efficiency and insights. Mavis is a CFA charter holder and holds an MBA from the University of Chicago Booth School of Business.



Peter Baciorowski, CISA, is a Managing Director at Deloitte specializing in auditing and building AI and digitally enabled solutions, grounded in Risk, Financial services, and Internal Audit. He has 18 years of experience managing both large- and small-scale data science solutions involving various machine learnings, data visualization, data warehousing, data transformation, profiling, trend analysis, reconciliation, and statistical sampling techniques. Pete leads analytics efforts to assess and mitigate risk as well as to support audit and consultative services in the testing of various business processes and controls environments. As Managing Director, Pete oversees growth and service delivery for all Consumer

Products audit clients, which also spans the Automotive and Retail sectors. He earned a Bachelor of Science in Computer Science and Engineering from Oakland University and is a Certified Information Systems Auditor.

2:15 – 3:15 PM: Closing the Cybersecurity Capability Gap: What Organizations and Internal Audit Keep Getting Wrong

Ryan Rene Rosado / Atom Cyber Advisory

Organizations cannot govern risks they cannot see. This session examines how sensitive data, unsanctioned AI tools, SaaS applications and third-party dependencies spread across the enterprise, and how continuous discovery, classification and evidence can help management and Internal Audit establish meaningful oversight.



Ryan René Rosado leads Atom Cyber Advisory, where she delivers strategic cybersecurity and risk advisory services to organizations navigating complex, evolving threat landscapes. She is a former Manager in RSM US's Cybersecurity Consulting Practice and Head Teaching Assistant at Harvard Extension School, supporting graduate-level cybersecurity courses. A U.S. Air Force veteran and former enlisted cyber intelligence analyst, Ryan brings nearly 15 years of experience across the public, private and academic sectors. Her expertise spans incident response, threat intelligence, risk management, compliance and cybersecurity education. She is also an advisor to Ally Security and a frequent speaker on cybersecurity workforce development, education and the cyber capability gap.

3:15 – 3:30 PM - Break

3:30 – 4:25 PM: Keeping Humans Accountable in an AI-Enabled Organization

Maura Charles – Founder & CEO; Keep it Human

Most of today is about what AI is doing. This session is about who answers for it. As agents take on real decisions, ownership quietly erodes and organizations build up moral debt: the hard calls about accountability and authority that never get made. Maura will show where human judgment must stay in charge, how to spot accountability gaps before they become audit findings, and the practical questions Internal Audit can ask to test whether AI operates within the organization's values, boundaries, and controls.



Maura Charles is the Founder and CEO of Keep it Human, a human-focused AI transformation firm that helps organizations adopt AI without losing track of who decides, who's accountable, and where human judgment must stay in control. She brings 25 years of Fortune 500 operating experience as a product leader and general manager at companies including Time Inc., Bloomingdale's, Allergan, and Cablevision. Maura works with executive teams to find where AI is quietly creating risk, clarify decision rights, and put human oversight where it belongs. A frequent writer and speaker on AI, leadership, and the future of work, she focuses on what organizations owe the people inside them as the technology moves faster than the rules.

4:25 – 4:30 PM: Conference Wrap Up

Final thoughts and suggestions on how emerging technology affects us today and how internal auditors can be best prepared for the future.