Opening Keynote: A New Approach to Data Privacy: 4 Pillars That will Form the Future

Daniel T. Yunker
Principal, Internal Audit Leader, Healthcare Consulting
Crowe LLP

Dirk Arends
Principal Consultant, Migration and Modernization
Amazon Web Services

Amanda Marderosian
Privacy and Data Protection Manager, Consulting Practice
Crowe LLP

With the rise of transformative technologies like big data, biometrics, genetic testing, and generative AI, inadvertently exposed sensitive data poses an increasing concern for corporations, government agencies, and nonprofits alike. How can internal audit help organizations maintain transparency, promote good governance, and operate with ethics, efficiency, and compliance in their race to safeguard their most precious commodity — data? In this keynote, Crowe will be joined by a representative from Amazon Web Services (AWS) to discuss emerging challenges and uncover a new 4-pillar approach that will help auditors ensure ethics, governance, cybersecurity, and privacy in a new frontier for data privacy shaped by AI, cloud computing, and other increasingly complex environments.

In this session, participants will:

- Uncover the most pressing issues facing internal audit today amidst the rise of transformative technologies.
- Discover the 4 pillars that will form the future of internal audit and help safeguard data.
- Learn applicable strategies they can apply on the job, today and tomorrow.
- Gain a new perspective on the importance of their role and how they can help change the conversation regarding internal audit.

Daniel Yunker is responsible for leading the strategic direction of Crowe Healthcare Internal Audit and Risk services and solutions, which includes more than 500 healthcare-specific professionals. He has helped develop new ways to add value for large healthcare systems and advance healthcare delivery in the communities served. Recognized as an industry thought leader, Yunker has held executive roles with

Northwestern Medicine, Loyola Medicine, Metropolitan Chicago Healthcare Council, Aon, and the Healthcare Financial Management Association.

Dirk Arends is a Principal Consultant on Migration and Modernization at Amazon Web Services, where he advises customers on the digital transformation journey. Previously, he oversaw cybersecurity, compliance, and governance as President and CTO at Virtual Systems.

Amanda Marderosian provides tailored support for data privacy and compliance leaders within a variety of regulated industries, including life sciences, manufacturing and distribution, and high-tech. In addition to leading projects focused on operationalizing privacy programs, she consults on complex compliance-related matters, configures privacy platforms, and conducts compliance assessments on internal policies for in-scope privacy regulations.

NASBA: Specialized Knowledge | Learning Level: Intermediate | CPE Credit: 1.8
Prerequisite: General knowledge of data privacy requirements

8:40–9:40 a.m. PT | 10:40–11:40 a.m. CT | 11:40 a.m.–12:40 p.m. ET

CS 1: Cybersecurity Risk Management Regulations: Regulatory Compliance and The Three Lines of Defense

Andy Watkin-Child, CEng, CSyP, MSyI, MIMechE, AMAEW
Founding Partner
The Augusta Group and Parava Security Solutions

Cyber is a significant national, economic, and societal security risk being regulated by both nation states and national regulators. U.S. and EU regulators have issued final cybersecurity regulations such as the SEC cyber rule (July 2023), EU NIS2, and EU Digital Operational Resilience Act (DORA) (January 2023), which have far-reaching effects on the oversight, assurance, and attestation of cyber risks for covered entities, their boards, and internal audit.

In this session, participants will:

- Explore the final cyber regulations finalized by the SEC, EU NIS2, and EU DORA; the effects of these regulations on covered entities; the importance of governance and the Three Lines of Defense; and internal audit's role in the oversight, assurance, and attestation of material cyber risk and material cyber incident disclosure with and on behalf of the board and board subcommittees.
- Examine significant cyber risk management regulations, disclosure reporting requirements, and the change from cybersecurity to cybersecurity risk management.
- Evaluate material cyber risks, required for Form 10-K and Form 20-F disclosures, which will be due beginning with annual reports for fiscal years ending on or after December 15, 2023.
- Discuss material cyber incident disclosures by U.S. domestic and International Foreign Issuers (Form 8-K and Form 6-K) due from December 18, 2023, including disclosures to be submitted four business days after a company determines that a material cybersecurity incident has occurred.

Andy Watkin-Child has 20 years of experience holding international leadership positions in the first and second lines for cybersecurity, cyber-risk management, operational risk, and technology within engineering/manufacturing, financial services, and publishing/media companies with balance sheets over €1 trillion. He is an experienced member of management boards, global risk leadership teams, and cybersecurity, operational risk, and GDPR committees. Watkin-Child is the Founding Partner of Parava Security Solutions, an independent cyber-risk management advisory firm that supports organizations in delivering cyber-risk management and cyber regulatory programs. He also runs CMMC Europe, an advisory company focused on

supporting the European Defence Industry Base (DIB) in deploying Cybersecurity Maturity Model Certification (CMMC).

NASBA: | Learning Level: | CPE Credit: 1.2
Prerequisite:

CS 2: Auditing The Data Privacy Program

Mark Thomas, CGEIT, CRISC, CDPSE, COBIT Assessor, ITIL, PRINCE2
President
Escoute Consulting

As corporations, governments, and non-profits identify and implement innovative ways to use data, their responsibilities for ensuring appropriate safeguards over the collection, storage, and destruction of data may be challenged. Additionally, as data is subject to emerging and changing regulatory requirements, those same challenges are heightened. This presentation will address the key aspects of privacy and how to create an audit/assurance program with control objectives in the areas of data privacy, from data collection all the way through incident management.

In this session, participants will:

- Understand the key definitions and concepts of data and information privacy.
- Recognize the key success factors to creating a privacy assurance program.
- Identify key control objectives that make up an audit and assurance program for privacy.

Mark is an internationally known Governance, Risk and Compliance expert specializing in information assurance, risk IT strategy and digital trust. With over 30 years of professional experience Mark has a wide array of industry experience including government, health care, finance and banking, manufacturing, and technology services. He has held roles spanning from CIO to IT consulting and is considered a thought leader in frameworks such as COBIT, NIST, ITIL and multiple ISO standards.

NASBA: Auditing | Learning Level: Intermediate | CPE Credit: 1.2
Prerequisite: General understanding of audit and data privacy concepts

CS 3: Data Governance in the Cloud

Booker (Tyrone) Showers
Partner
Taliferro

Booker (Tyrone) Showers is a Partner at Taliferro Group. A visionary leader, he possesses technological acumen as well as a deep understanding of people, passions, and potential. His strengths include analyzing business operations, optimizing processes, designing comprehensive growth strategies, and strategically aligning technology with vision to enable both startup and established enterprises to discover new energy and purpose, maximize opportunities, and reach new pinnacles. Showers takes pride in personal connections, sees beyond balance sheets and technology stacks, and understands that at the core of every business lies human ambition and dreams.

NASBA: | Learning Level: | CPE Credit: 1.2
Prerequisite:

CS 4: The Evolving Role of IT Audit: Preparing for Regulatory Changes and Emerging Technologies

Dr. Lisa McKee
Partner
American Security and Privacy

The IT audit role is constantly evolving as new laws and regulations are passed globally. Technological advances, AI, and emerging technologies impact how auditors assess systems, applications, and processes for risk related to data processing and compliance. It is important for IT auditors to assess security and privacy controls to protect organizations against threats related to emerging technologies and privacy cyberwarfare.

In this session, participants will:

- Examine changes in the regulatory landscape.
- Consider the impact of AI and how to protect data in organizations.
- Get tips on auditing security and privacy controls.
- Construct an IT audit plan for emerging technologies and privacy cyberwarfare.

Dr. Lisa McKee is a Founding Partner at American Security and Privacy, LLC. She has 20+ years of industry experience and provides virtual Data Protection Officer (vDPO) services, including assessments, training, program development, and leadership, for companies internationally. She completed a Ph.D. in Cyber Defense with a dissertation in Privacy from Dakota State University. A highly regarded privacy expert, she has spoken at global events held by IAPP, ISACA, The IIA, and RSA. She is a member of the Accredited Standards Committee X9 and an APMG ISACA Certified Trainer. Dr. McKee volunteers on boards for several professional groups, mentors and teaches graduate students as an adjunct professor at several universities, and has authored several publications and a data privacy management textbook.

NASBA: Auditing | Learning Level: Intermediate | CPE Credit: 1.2
Prerequisite: General understand of auditing technical controls for regulatory compliance