



7:00 – 8:30 AM PDT | 9:00 – 10:30 AM CDT | 10:00 – 11:30 AM EDT

**Opening Keynote: Auditing Data Privacy Practices to Achieve Value-add**

**Leeza Garber, J.D.**  
**Adjunct Law Professor**  
**Drexel University, Kline School of Law**

In the midst of evolving cybersecurity threats, massive data collection, and extended remote work capabilities, audit executives must address data privacy practices head-on. Every organization relies on data to run its business: whether it's customer contact and payment information, or granular updates on how products move through a supply chain. Data privacy laws vary across industry, and federal and state requirements are constantly changing, with impactful legislation proposed every month. Determining what data privacy practices are in place, critically analyzing them, and determining whether they meet the relevant standards is not only a dynamic task, but one that should create value for an organization.

In this session, participants will:

- Learn about the major state and federal laws that impact data privacy across a variety of sectors, including finance, retail, healthcare, and government.
- Appreciate what best practices are for holistic data privacy, and how obligations are evolving.
- Understand what threats to data privacy exist and target their employer, so data privacy practices can be customized and vulnerabilities patched.
- Be empowered to explain how data privacy is inextricably bound to all elements of the daily operation of most businesses, and how to showcase to the C-suite (and beyond) why consistent audits are not only necessary, but add serious value across the board.

**Leeza Garber, Esq.** is a cybersecurity and privacy attorney and consultant. She is an award-winning lecturer at The Wharton School, University of Pennsylvania, teaching Internet Law, Privacy, and Cybersecurity, and is also an adjunct law professor at Drexel University's Thomas R. Kline School of Law focused on information privacy. Appearing as an on-air expert for Fox News Channel, Fox Business Network, and the National Desk, Garber analyzes cybersecurity, privacy, social media, and tech-related news. She has been published in *Newsweek*, *The Hill*, and *Wired*, and she co-authored a book with former FBI agent Scott Olson, *Can. Trust. Will.: Hiring for the Human Element in the New Age of Cybersecurity*.



8:40 – 9:40 AM PDT | 10:40 – 11:40 AM CDT | 11:40 AM – 12:40 PM EDT

**CS 1: Understanding the Evolving Regulatory Environment on Data Privacy and Protection**

**Greg Anderson**  
**Vice President, Chief Privacy Officer**  
**The E.W. Scripps Company**

Recent GDPR and California Consumer Privacy Act mandates were both designed to protect privacy and data in the strictest means possible. During 2021, new state-level data privacy regulations included the Virginia Consumer Data Protection Act, the Colorado Privacy Act, and others. Are your organization’s initiatives keeping pace with increased regulations? As organizations gain experience in developing and implementing privacy frameworks, how can internal audit expand its involvement in the critical area of risk?

In this session, participants will:

- Learn about the latest regulations related to data privacy and protection.
- Understand the responsibilities of the CIO/CISO in data privacy and protection.
- Explore how internal audit can take a more active role in helping organizations develop more effective privacy policy and programs.

**Greg Anderson** has built multiple compliance programs, led hundreds of complex technology transactions, and managed mobile network deployments around the world. He is currently the Chief Privacy Officer for The E.W. Scripps Company. In May 2020, Anderson joined the advisory board of SuriData.ai. He is CIPP-E certified and holds law degrees from the Université Jean Moulin and the University of Georgia.



9:50 – 10:50 AM PDT | 11:50 AM – 12:50 PM CDT | 10:00 – 11:30 AM EDT

## CS 2: Executing the Mindset Change: Internal Audit’s Role in Operationalizing and Monitoring Privacy Risk

**Adam Pajakowski**  
Consultant  
Crowe

**Josh Reid, CGMA, CPA**  
Principal, GRC Technologies Practice Leader  
Crowe

This presentation will leverage prior webinars and thought leadership articles to recap areas of top risk related to privacy for internal auditors.

In this session, participants will:

- Gain a detailed understanding of how internal audit can be a business partner in some top risk areas related to privacy.
- Explore how an integrated risk management approach can help internal auditors monitor and manage privacy risk.
- Discuss how a risk and performance monitoring technology can be leveraged by internal audit.

**Adam Pajakowski** is engaged in all aspects of Crowe’s data privacy solution as a member of the Privacy and Data Protection core team. His experience encompasses regulation-based audits, privacy audits, data transparency audits, and readiness and gap assessments. As a leading member of Crowe’s Third Party Risk Management solution, he also has deep experience in assessing risk in key third parties for organizations. Pajakowski’s 14+ years of experience spans the manufacturing, life science, healthcare, and construction industries and includes projects in internal audit, SOX, ERM, compliance, and third-party vendor reviews. He focuses on services for pre-/post-IPO clients and leads projects around risk, governance, and compliance for high-growth companies. Pajakowski has developed deep expertise in identifying risk and developing new audit programs for complex processes.

**Josh Reid** is a Principal in Crowe’s Consulting Life Sciences Practice and serves as Crowe’s firmwide Governance, Risk, and Compliance (GRC) Technologies solution leader. With 18+ years of experience, he focuses on leading risk management and compliance software implementation projects, encompassing enterprise risk management, cybersecurity, third-party risk management, internal audit, business resiliency, and regulatory compliance. Reid’s responsibilities include overseeing the strategic direction of Crowe’s GRC Technologies solution offerings, enhancing Crowe’s proprietary GRC SKILL implementation methodology, and bringing new risk management solution offerings to market. He has worked closely with leading risk management technology platforms, including Archer, SSIC X-Analytics, Onspring, NAVEX IRM, OneTrust GRC, and BWISE.

NASBA: Auditing | Learning Level: Beginner | CPE Credit: 1.2



11:20 AM – 12:20 PM PDT | 1:20 PM – 2:20 PM CDT | 2:20 PM – 3:20 PM EDT

### CS 3: Internal Audit’s Role in Data Privacy: Leveraging BCR and SaaS Transformation

**Derek Thomas, CISA**  
Senior Director, Enterprise Risk Management and Internal Audit  
Hewlett Packard Enterprise

**Felipe Castro, CISA, CRISC**  
Manager, Cybersecurity Internal Audit  
Hewlett Packard Enterprise

The remote workforce brought on by the pandemic has limited face-to-face contact and companies’ ability to monitor employee productivity. It has also amplified digital shifts and privacy risks for many companies, as centralized management of cloud technologies and software as-a-service (SaaS) – often embedded in legal organizations – is now stratified across digital delivery teams. How can companies in an SaaS transformation address this challenge effectively and how far does internal audit’s role extend in overseeing privacy risk? This session will share how the Binding Corporate Rules (BCR) framework created an opportunity for internal audit and legal privacy to integrate in developing an effective go-to-market oversight model for a large, decentralized organization.

In this session, participants will:

- Understand how digital transformation accelerates global privacy risks.
- Examine the role of internal audit in legal privacy programs and clarify the level of knowledge and experience needed to execute internal audit’s oversight role.
- Learn about general considerations to include in their privacy audit risk planning.
- Hear how general privacy controls can be shared across multiple oversight functions.
- Differentiate the security triad and core privacy principles and where they overlap.
- Share an initial foundation for the incorporation of privacy audits into a global audit plan.

**Derek Thomas** is a Senior Director in HPE’s Internal Audit and ERM organization, based in Portland Oregon. He joined HPE in 2019 to lead the cybersecurity and technology audit teams and recently transitioned to lead Enterprise Risk Management. Thomas previously spent 12 years with Deloitte in their Enterprise Risk Services organization, consulting in security, assurance, and risk management, before joining NIKE’s information technology organization to lead the information risk management and security compliance program. He maintains a Certified Information Systems Auditor (CISA), Certified Data Privacy Systems Engineer (CDPSE) and ISO 27001 Sr. Auditor certifications.

**Felipe Castro** is a Cybersecurity Audit Manager in the Guadalajara, Mexico HPE Office with 24 years of information technology, audit, and information security experience. He is a frequent presenter on cybersecurity auditing techniques with a focus in cloud security and vulnerability controls. Castro has also contributed to the Cloud Security Alliance (CSA) Certified Cloud Auditing Knowledge (CCAK) development. He has obtained multiple certifications, including ISACA’s Certified Information Systems Auditor (CISA) and Certified in Risk and Information Systems Control (CRISC).

NASBA: Specialty Knowledge | Learning Level: Intermediate | CPE Credit: 1.2



12:30 – 1:30 PM PDT | 2:30 – 3:30 PM CDT | 3:30 – 4:30 PM EDT

#### CS 4: Data Privacy and Ethics: Why Does It Matter?

**Robert S. Jett III**  
**Chief Privacy Officer**  
**Crawford & Company**

As organizations gain experience in designing and implementing privacy, data protection, and compliance strategies to address new and updated regulatory, operational, and business risks, how can internal audit expand its involvement related to data management? Is your organization reviewing the principles around the ethical use of data? Does your organization ask the proper questions related to data collection, use, and retention?

In this session, participants will:

- Gain an understanding of how internal audit can be a business partner on data privacy and protection issues.
- Examine principles around data ethics and making data-driven decisions for your organization.
- Review biases in algorithms and their potential impact on automated decision-making.

**Robert S. Jett III (“Bob”)** serves as Chief Privacy Officer and lead IT counsel for Crawford & Company. He has experience as a legal advisor and in-house counsel with multinational organizations in the medical device, insurance, and financial services industry and has worked closely with colleagues and issues related to information technology, data privacy and protection, information security and corporate compliance functions. This has included the creation, implementation, and maintenance of global compliance, incident response, and data privacy programs as well as the management of a global privacy office for several global companies.

NASBA: Behavioral Ethics | Learning Level: Beginner | CPE Credit: 1.2