Innovation Session 701 Sponsored by Vanguard Integrity Professionals: How Does Continuous Monitoring And Compliance Enforcement Fit Into GRC And Why Do We Need It?
Virtual Attendees Only. No CPE Credit

John Connors
Vice President of Technology
Vanguard

A well-planned GRC strategy comes with lots of benefits: improved decision-making, more optimal IT investments, elimination of silos, and reduced fragmentation among divisions and departments, to name a few.

After completing this session, attendees will be able to:
• Establish a very specific plans for remediation to close “gaps”
• Leverage proven tools that constantly evaluate the status of your environment
• Establish and use very specific policies that are enforceable for access rights
• Control excess access & access rights to critical data – review constantly
• Implement continuous monitoring and enforcement of access policies"

John joined Vanguard’s Professional Services Team as a Senior Professional Services Consultant in April 2002 and has amassed over 35 years of cybersecurity experience. Connors has a broad based technical background with expertise and certifications including Microsoft Certified Systems Engineer (MCP, MCP+I, MCSE), Cryptographic System Repairman, Computer Languages including .NET, C#, C++, ADA, PHP, Visual Basic, HTML, SQL, Perl, Dbase III, ACCESS; CISCO Firewalls, Switches, Routers, Frame Relay, ATM, Microsoft Information Server, Microsoft SQL Server, Microsoft Site Server, VTEL Video Communications Systems, TC2000, Multi-point Conference units, AT&T Switches, Dimension 400, 2000, System 75/85 and G3.

Opening Keynote: Pivot Point: Thriving in Crisis for Systems and Audit

8:30 AM – 9:45 AM
NASBA Field: Auditing
Learning Level: Intermediate

Shawn Rhodes
TEDx Speaker, Nationally Syndicated Columnist
In the world of governance, risk and compliance, the best plans may not always unfold as expected. To address the constant challenge of adapting to COVID and its effects on our businesses, keynote speaker Shawn Rhodes credits his experiences as a Marine Corps war correspondent and as a consultant to businesses in more than two dozen countries for sharpening his insights and preparing for the unexpected. He will share how the best teams and organizations across industries pivot to leverage change when it occurs, build engaging cultures and ensure the experience of senior leaders doesn’t leave when they do.

Shawn Rhodes leveraged his former life as a war correspondent to become an international expert in how to pivot when change enters our plans. He is a Tampa-based TEDx speaker and his work studying teams in more than two dozen countries - some the most dangerous places on the planet - has been published in news outlets including TIME, CNN, NBC, Forbes, the Wall Street Journal and INC. His clients have included Deloitte, ConAgra, Coca-Cola, and dozens of similar businesses. Shawn is also a nationally syndicated columnist with the Business Journals and author of the books Pivot Point: Turn on A Dime Without Sacrificing Results, Universal Export: A Guide for Overachievers in Working Less And Enjoying More, and forthcoming book, Bulletproof Selling: Surviving And Thriving On The Battlefield Of Sales.

Innovation Session 702: Common Considerations and Challenges in Adopting a New GRC Platform
9:50 a.m. – 10:10 a.m.
Virtual Attendees Only. No CPE Credit

Todd Fitzgibbon
GRC Offering Lead
OneTrust GRC

How much time do you spend transferring data across systems and spreadsheets to execute your GRC program? Oftentimes, disparate systems across policy, privacy, IT risk, vendor risk, incident, and audit result in duplicated data across applications. There is no such thing as a one-size fits all solution in GRC, teams want a specialized tools that can adapt to their unique functional needs. Join this session to learn common considerations and challenges in adopting a new GRC platform. We'll discuss how to bring the elements of an integrated GRC program together under one roof, from mapping your business scope, to auditing and reporting on operations.

After completing this session, the participant will be able to:
• Review how to execute the core functions and controls within ISO 27002 ISMS guidelines
• Balance the scales between integration and system adoption – delivering priorities across teams
• Identify key data sets where you can prioritize integrations between modules or applications
• Reduce manual data transfers to streamline evidence collection for audit analysis and reporting
Todd Fitzgibbon serves as GRC Offering Lead for OneTrust GRC—a purpose-built software designed to operationalize integrated risk management. In his role, Todd is responsible for driving the development and delivery of OneTrust's integrated risk management product as well as driving the refinement of the tool-set and offerings. He advises companies throughout their risk management implementations to establish processes to support operations and align with their enterprise objectives, including adopting industry best practices and adhering to requirements relating to relevant standards, frameworks, and laws (e.g. ISO, NIST, SIG and more). Todd works with clients to realize the extent of their risk exposure, helping clients to map their digital infrastructure, assess risks, combat threats, monitor ongoing performance, and document evidence throughout the risk lifecycle.

CS1-1: Why Is Vulnerability Management Still Such A Difficult Win?
10:10 AM - 11:10 AM
NASBA Field: Information Technology
Learning Level: Intermediate

Susanne Senoff, CISA, CISM, CRISC
Senior Director, Enterprise Security
Arm

Stuart Robbins
Senior Manager
Arm

Achieving visibility into the vulnerabilities in your environment and then driving action is a difficult challenge for most companies. In this session, we will discuss our experience with getting to 100% infrastructure visibility and successfully partnering with the organization to lower the risk. Key topics include:

- How to overcome organizational challenges
- How to use data to drive change
- What technology and platforms can be most useful?

After completing this session, the participant will be able to:

- Strategies to increase and measure visibility of vulnerabilities in their environment.
- Gain knowledge about technologies that can be deployed to lower vulnerability risk.
- Discuss how to overcome organizational challenges to lowering vulnerability risk.
- Approaches to reducing the cycle time for patching their environment.
Susanne Senoff joined Arm in 2018 where she started up the Enterprise Security Governance, Risk, and Compliance function. In this role, she leads risk management, vulnerability management, training and awareness, security measurement and remediation. Prior to Arm, Susanne held director level positions at Microsoft and Morgan Stanley. She was also a management consultant, consulting on building security programs for companies ranging from 9-person start-ups to multi-billion dollar companies.

Stuart Robbins is the Senior Manager of Governance & Remediation at Arm, where he has led the development of Arm’s Threat & Vulnerability Management function. He has worked in a variety of Technical, Information Security and Risk Management roles across Security Architecture, Engineering and Operations. He has over 20 years of Information Technology and Cybersecurity experience in Technology and Professional Services Industries in the UK, Europe and the US.

**CS1-2: A Practitioner’s Guide to Technology Risk and Control Evaluation**  
10:15 AM - 11:15 AM  
NASBA Field: Auditing  
Learning Level: Intermediate

David Muxfeld, CRISC  
First Vice President and Director, IT GRC  
Federal Home Loan Bank of Atlanta

Risk and control evaluation is the keystone of a functional risk management framework. However, it can be a challenge to perform them effectively, even for experienced practitioners. Join me as I walk through a hypothetical cybersecurity attack and a troubled space journey to Mars to demonstrate some core elements of effective risk and control analysis and what may happen when they are done poorly.

**After completing this session, the participant will be able to:**

- Describe the criteria for effectively performing risk and control analysis.
- Map mitigating controls to identified vulnerabilities.
- Interpret evaluation results to determine risk impacts and control efficacy.

David Muxfeld is an IT Governance, Risk, and Compliance leader with over 15 years of experience assessing enterprise risk and information security control mitigations for organizations in the insurance and financial services industries. Dave has successfully designed and implemented various organizational technology assurance strategies and has held various industry certifications including Certified Ethical Hacker, Certified Information Privacy Technologist, and Certified in Risk and Information Systems Control.
The hype surrounding artificial intelligence (AI) is everywhere, however many ignore one of the looming challenges today: governance. In the race towards AI adoption, organizations face a "shadow AI" problem—without knowing how to regain control. This presentation will identify the signs of shadow AI and give attendees practical tips for establishing AI governance. Attendees will leave empowered with an understanding of how to best measure and monitor the success of their AI initiatives.

After completing this session, the participant will be able to:

- Understand the risks associated with shadow AI and the steps needed to regain control for their organizations. Shadow AI is the proliferation of AI-enabled tools or applications by groups or individuals without any IT or security oversight or governance. A direct result of the democratization of AI, shadow AI generally stems from well-intentioned teams. However, corrective actions must be taken now to mitigate any potential risks.
- Receive practical, step-by-step guidance for establishing an effective AI governance function. We will share tips to help reduce risks while encouraging innovation and providing teams the right tools to better monitor the success of their AI initiatives. Find out how a centralized solution for AI processing and governance can address many of the issues stemming from shadow AI while improving collaboration amongst all stakeholders (e.g., data scientists, development teams, IT and business leadership). Looking for better control over AI initiatives and systems? We’ll use a case study to discuss how.
- Learn how establishing a centralized, embedded, approach to governing AI solutions enables better monitoring for AI initiatives. We’ll walk through the metrics data scientists and development teams should be monitoring to ensure models remain accurate and performant when in use in IT systems and applications. We will also share the metrics all leaders should establish to monitor the ongoing performance and success of their AI programs.
Kirsten Lloyd is Head of Go-to-Market at Modzy®, the ModelOps platform to integrate, monitor, and secure AI models at scale. She has authored and contributed to numerous reports on the intersection of ethics and AI, including Bias Amplification in AI Systems, Assessing the Ethical Risks of Artificial Intelligence, and A National Machine Intelligence Strategy for the United States. She is also an accomplished speaker having presented at NVIDIA GTC, the AAAI 2018 Fall Symposium, ISACA’s 2018 Governance, Risk, and Controls conference, Stanford’s inaugural Digital Cities Summit in 2016, and more.

CS1-4: Agile Audit Communication – Better audit results. More added value.
10:15 AM - 11:15 AM
NASBA Field: Auditing
Learning Level: Intermediate

Tracie Marquardt, CPA
Internal Audit Communication Consultant

Internal Audit is going Agile. Or is it? Many audit teams, many companies, just aren't ready for it. Experience tells us the key to the success of agile project methodology is communication: It's flexible. It motivates. It brings accountability and transparency. So how can Audit harness the benefits of agile communication without (necessarily) adopting agile project methodology? Is your team ready to break free from traditional audit communication practices?

After completing this session, the participant will be able to:
• Distinguish between Traditional communication and Agile communication
• Explore Agile communication concepts for Audit
• Identify the risks of adopting Agile communication concepts
• Examine what it means to apply Agile audit communication in your team

Tracie Marquardt is Europe’s leading audit communication specialist, empowering international Internal Audit executives and their teams to become more effective in their global communication. Tracie is passionate about inspiring audit professionals to be more, do more and create more through positive communication. Her strategic approach addresses the heart of audit’s challenges: to derive and communicate results that add more value to stakeholders, positively impacting the organization’s productivity and profitability. She is a CPA and Deloitte alumn with a degree in Chartered Accountancy from the University of Waterloo in Canada. She is a club Past President and active member of Toastmasters International.
In the past 18+ months companies have had to make so many changes so quickly—often with startling success—that leaders have every reason to believe they can do even more. Of course, the risk surface we were defending just a few years ago have changed drastically and the threats are more pervasive than ever. Many companies are sweating the details of their return plans rather than building the capabilities needed for a return. Now is the time for risk managers and cybersecurity professionals to re-examine how we look at the assets we are defending, adjust how we look at risk and bring new strategies to bear on the challenges we face. Join Chris Patteson as he shares his thoughts on this topic and explores concepts to address these challenges.

Chris Patteson has more than two decades experience as a practitioner, leader, and innovator within Governance Risk and Compliance and Integrated Risk Management in the manufacturing, technology, and logistics sectors. Prior to joining RSA, he managed a team of data scientists and application developers to build new methods, models, and architectures for managing fraud and cargo security for a global logistics organization. Chris continues to drive innovation in advanced data modeling techniques and creating actionable intelligence for managing risk.
This presentation examines current and future state GRC alignment models and advocates for GRC to hold a central position in executing business goals, responding to audit and regulatory inquiries, and mitigating security threats. By exploring an expanded alignment of requirements beyond the traditional model, GRC can strengthen and unify a firm’s security and risk posturing.

After completing this session, the participant will be able to:

- Understand the current state of GRC models and the pressures to modernize the traditional alignment.
- Explore an expanded GRC alignment model and the steps to build it.
- Recognize how an expanded GRC alignment model can assist in achieving business goals, responding to audits and regulatory inquiries, and mitigating threats.
- Learn strategies to advocate and scale an expanded GRC alignment model at their firm.

Jack Swearingen is the Manager of the Security Policy and Governance team at Coinbase, a leading cryptocurrency exchange platform dedicated to building a more fair, accessible, efficient, and transparent financial system enabled by crypto. Jack began his foray into cybersecurity and information assurance working at an international law firm, and then moved into securing large financial institutions, working in a variety of roles in both the first and second line. He has seen firsthand the tremendous benefits of robust GRC practices, and continues to successfully advocate for GRC’s central role in business decisions and security practices. Jack holds Bachelor of Arts degrees in Political Science and International Studies, with a specialty in East Asian politics, from Southern Methodist University, and a Master of Engineering in Cybersecurity Policy and Compliance from George Washington University.

CS2-2: Vendor Risk - Giving Away Your Keys To The Kingdom
11:30 AM - 12:30 PM
NASBA Field: Business Management & Organization
Learning Level: Beginner

Brian Murphy, CISA, CRISC
Senior Security Specialist
GreyCastle Security

As we have seen time and time again, cybercriminals take the path of least resistance. They have learned that contractors and other third-party providers can provide an opening into otherwise-secured corporate networks. You have spent time, money, & energy securing your organization internally, only to have the back door wide open. Learn what is working, what is not, and how your organization can better manage one of the most challenging security issues facing organizations today.

After completing this session, the participant will be able to:

- Identify third-party vendors that should be managed.
- Develop a prioritized, actionable plan for vendor risk mitigation.
- Address common third-party challenges and how to overcome them.
Brian Murphy is a technology, information security, and risk management professional. He has been at GreyCastle Security since 2018 and over 10 years of professional experience assisting with the development and implementation of cybersecurity solutions for financial services, healthcare, higher education, energy, information technology, and manufacturing industries. He has knowledge of PCI, SOX, GLBA compliance requirements, and ISO and NIST standards and regulations that can be applied in a variety of functions.

**CS2-3: The Power of Analytics in Internal Audit**

11:30 AM - 12:45 PM  
NASBA Field: Information Technology  
Learning Level: Beginner

Jenna Caprara  
Internal Audit Manager  
AARP

Matthew Leister, CISA  
IT Internal Audit Manager  
AARP

Big data is a common buzz word in the Internal Audit industry. Most auditors see the focus on analyzing client data for testing. This session will not only delve into analyzing and visualizing data but also show you ways to use analytics and visualizations to perform an annual risk assessment and manage audits within the internal audit function.

**After completing this session, the participant will be able to:**

- Learn why analytics are important to the internal audit function.
- Demonstrate ways to analyze and visualize data for the annual risk assessment, audit scoping, testing, and reporting.
- Demonstrate ways dashboards can be used to improve audit execution, communication, and customer experience.

Jenna Caprara has been an Internal Audit Manager at AARP for seven years focused on financial, operational, and compliance. She has audited various processes including privacy, procurement, media buying, ERM, and digital transformation implementations to name a few. Her past experience includes five years working as an external auditor at RSM US.

Matthew Leister is a Virginia Tech graduate with seven years of experience consisting mostly of Internal Audit, External Audit, Grants Compliance, and Advisory projects. Matt started his career in Public Accounting where he provided a variety of services which included both IT and Business Process Internal Audit, External IT Audit (SOX), Reg AB and SOC audits, and also project management consulting. After working as a Senior IT Internal Auditor for a major insurance company, Matt joined AARP in his current role as an IT Internal Audit Manager.
Shawn Rhodes
TEDx Speaker, Nationally Syndicated Columnist

In the world of governance, risk, compliance, and audit, the best plans never work out as planned. As an addendum to his keynote, Shawn will dig deeper into the constant challenge of implementing new ideas and ensuring past mistakes aren't repeated. He will walk audience members exactly how to build a change-friendly plan to:

- Develop clear objectives for each employee on every project
- Identify the most likely changes they'll encounter along the way
- Find solutions before problems affect results
- Incorporate the experience and wisdom of senior leaders
- Debrief results so every project is better than the last
- Establish effective communication protocols with audit customers.

Shawn Rhodes leveraged his former life as a war correspondent to become an international expert in how to pivot when change enters our plans. He is a Tampa-based TEDx speaker and his work studying teams in more than two dozen countries - some the most dangerous places on the planet - has been published in news outlets including TIME, CNN, NBC, Forbes, the Wall Street Journal and INC. His clients have included Deloitte, ConAgra, Coca-Cola, and dozens of similar businesses. Shawn is also a nationally syndicated columnist with the Business Journals and author of the books Pivot Point: Turn on A Dime Without Sacrificing Results, Universal Export: A Guide for Overachievers in Working Less And Enjoying More, and forthcoming book, Bulletproof Selling: Surviving And Thriving On The Battlefield Of Sales.
Keeping pace with compliance obligations and subjective interpretations of risk has been a common barrier across the three lines. Chasing the latest information across static assessments, emails, and other documentation is inefficient and leaves you reviewing yesterday's data. Managing risk and compliance collaboratively across the three lines is essential for your GRC program to work effectively but can be challenging to execute.

In this webinar, we'll discuss how you can avoid risk blind spots and meet the first line where they operate. Using today's technology, audit & risk professionals can collect insights directly from the source in real-time, leveraging automated assessments, system integrations, while using their risk methodology. Making it possible for businesses to integrate risk management into business operations and eliminate traditional silos and specialty domains.

After completing this session, participants will be able to:

- Identify where you can extend GRC touchpoints to your first line without forcing them to adopt a new system
- Present risk management in context to the business to translate beyond traditional, but subjective risk inquires
- Reduce the lag in data collection and increase confidence in your risk analysis.

Sam Parker serves as a GRC Solutions Engineering Manager for OneTrust GRC – a purpose-built software designed to operationalize integrated risk management. In his role, Parker advises companies throughout their risk management implementations to establish processes to support operations and align with their enterprise objectives, including adopting industry best practices and adhering to requirements relating to relevant standards, frameworks, and laws (e.g. ISO, NIST, SIG and more). Parker works with clients to realize the extent of their risk exposure, helping clients to map their digital infrastructure, assess risks, combat threats, monitor ongoing performance, and document evidence throughout the risk lifecycle.
Audit fatigue is a symptom of the growing IT risk management burden that organizations face today. They must demonstrate compliance with a staggering list of information security standards that cut across both the public and private sectors, requiring a considerable amount of time, energy, cost, and expertise. This session focuses on the various issues that arise from having to support multiple compliance regimes. It will also discuss the findings of a recent research study conducted of 300 IT security professionals from the financial services, IT, energy, and other commercial sectors on the challenges they face when managing IT security and privacy audits.

In this session, participants will learn about:
- The impact that the growing number of security and privacy regulations has on organizations and individuals
- The unique compliance challenges presented by moving to the cloud
- The financial and productivity costs of IT security compliance to businesses
- Solutions for fixing the audit fatigue problem

Joining Telos in 2006, Steve Horvath established a new model for providing professional services in support of the company’s Xacta risk management platform. He currently serves as Vice President of Strategy and Cloud with a focus on long-term strategic partnerships and solutions spanning the company’s breadth of offerings. With over 20 years practical experience in the information security domain, Steve is considered an expert in risk and compliance for information technology. He is a graduate of the University of Maryland, College Park, and maintains the Certified Information Systems Security Professional (CISSP) certification.
Knowledge Session 803 Presented by Reciprocity: The Art of Compliance: How to Build A Defensible Compliance Program
12:50 PM - 1:20 PM
Virtual Attendees Only. ISACA 0.5 CPE

Rob Ellis
Senior Vice President of Strategy
Reciprocity

Scott McCormick
Chief Information Security Officer
Reciprocity

When it comes to doing business, being compliant is table stakes. Aside from the obvious necessity of a regulatory framework, it also helps foster a culture of compliance and ethics across your organization — an imperative for minimizing the potential risks and exposures from internal and external sources. But not all compliance programs are created equal. There’s a big difference between check-the-box annual or biannual compliance and defensible compliance, which empowers organizations to quickly and accurately understand the data they control, where it exists and how to properly secure, access, and manage it. Yet elevating GRC defensibility doesn’t have to be dauntingly complex. In fact, it can be as simple as leveraging a fully integrated and automated technology solution and taking five key steps. Join Reciprocity CISO Scott McCormick and SVP of Sales Rob Ellis as they break down what defensible compliance is, why you need it, and how to build GRC defensibility in your organization.

During this event they will discuss
- Moving to a zero-trust model
- Why certifications are just the start
- How automation future-proofs for change
- Reframing the narrative from a cost center to profit protector/business enabler

Rob Ellis has more than 15 years of experience leading sales, business development and marketing at SaaS startup companies. At Reciprocity, Rob is responsible for overall revenue growth. One of the company’s first employees, Rob was instrumental in scaling the business from zero - signing up Reciprocity’s first 40 clients, and building the sales and marketing organizations. A startup veteran, Rob has founded companies, and worked in venture-backed startups in a variety of roles including Director of Product at Veetle Inc.; Founder and VP, Product at NotchUp; and Director, Business Operations and Strategic Planning at Peerflix. Rob graduated from Cornell University with a BA in Genetics.

Scott McCormick is an InfoSec and GRC expert at Reciprocity. Scott brings over 20 years of experience to Reciprocity’s in-house expert advisory team. Prior to Reciprocity, Scott led security compliance at HackerOne.
Innovation Session presented by Fastpath: Modeling User Profiles for Your Transformation to the Cloud
1:25 PM – 1:45 PM
Virtual Attendees Only. No CPE Credit

Neil Hooper
Senior Vice President of Sales and Marketing
Fastpath

Liz Piteo
Solutions Architect
Fastpath

Fastpath’s Liz Piteo, Solutions Architect, and Neil Hooper, SVP of Sales and Marketing discuss new techniques for performing risk analysis when moving to a new ERP, Procurement, or HCM system in the cloud and how to manage and automate segregation of duties and access certifications enabling your continuous compliance.

In this session, participants will learn about:
- Understand new techniques for your security architecture and performing risk analysis in your ERP, Procurement, CRM or HCM systems
- Review how to manage and automate segregation of duties and access certifications enabling your continuous compliance
- Review compliant user provisioning for preventative controls
- Gain cross-application visibility to ensure controls through an entire process even if it crosses different systems

Neil Hooper is Fastpath’s Senior Vice President of Sales and Marketing. In this role, he is responsible for the company’s go-to-market organizations and continued record-setting growth. Prior to Fastpath, Neil grew successful global programs in GRC and InfoSec at companies including SAP, Rsam, Good Technology, and Motorola. With a proven track record in sales, marketing, and channel partner management, he has a unique perspective that includes experience running global operations while living and working in the UK, Switzerland, Belgium, Canada, Silicon Valley, and New York.

Liz Piteo holds a CRISC and is responsible for Fastpath’s pre-sales program and acts as a liaison between the sales and product teams. Prior to joining Fastpath, Liz had the distinction of being Fastpath’s third customer as well as working as a financial systems analyst responsible for SOX compliance and ERP security at several publicly traded South Florida organizations.
CS3-1: An Agile Approach to Auditing IT Controls
1:45 PM - 2:45 PM
NASBA Field: Auditing
Learning Level: Intermediate

Toby DeRoche
Owner
Insight CPE, LLC

Audit leaders are ready to implement an agile audit process in their departments, but nearly all of the support in the world is theoretical. This presentation provides audit leaders a guided discussion into a real-world case study of an IT Control department. The speaker will present the case and facilitate an open conversation about the merits and challenges of adopting an agile approach versus maintaining a traditional audit approach.

After completing this session, the participant will be able to:
- Discuss current challenges in scoping control testing.
- Apply agile principles to ITGC and Application control auditing.
- Analyze a real-world example with IT control testing difficulties.
- Debate the traditional versus agile approach benefits in this case.

Toby focuses his career advising governance and assurance professionals on solutions to their audit, risk, and compliance needs. As a credentialed subject matter expert, Toby assists organizations improve their internal audit, risk management, and compliance functions. He is also an experienced author and presenter, having delivered nearly 100 presentations to audit, risk, and fraud professionals.

Toby is a Certified Internal Auditor (CIA) with an MBA and Internal Audit specialization from Louisiana State University. He is also certified in Agile Audit (cAAP), SAFe Agile (SA), Control Self-Assessment (CCSA), Risk Management Assurance (CRMA), Internal Control Auditing (CICA), and Fraud Examination (CFE).

Toby's professional background includes over 15 years in internal audit, fraud examination, and technology enablement consulting. He is also an experienced speaker and prolific writer having delivered 16 whitepapers, 40 blogs, and nearly 100 presentations on audit, risk, and fraud topics. As the founder of Insight CPE, LLC, Toby is dedicated to audit, risk, and fraud professionals' continued education. In this role, he partnered with cRisk Academy to create the Certified Agile Auditor Professional (cAAP) course, the first of its kind in the world. As an audit and SOX consultant with RGP, Toby also puts theory into practice.
CS3-2: Defending Your Supply Chain
1:30 PM - 2:30 PM
NASBA Field: Information Technology
Learning Level: Intermediate

Alex Holden
CISO
Hold Security, LLC

Everything is a part of a supply chain. As hackers continue their assault against our supply chain, we will learn from past and present events about the true vulnerabilities and remediation steps. What can you do to secure your supply chain? The cyber threat landscape evolved beyond your supply chain securing itself, today each one of us should be invested in ensuring that our supply chain is secure.

After completing this session, the participant will be able to:
- Learn about history of supply chain security.
- Learn about attack patterns against the supply chain.
- Get practical advice of security your supply chain.
- Learn from practical examples on detecting and fixing security issues within your supply chain.

Alex Holden is the founder and CISO of Hold Security, LLC. Under his leadership, Hold Security played a pivotal role in information security and threat intelligence, becoming one of the most recognizable names in its field. Holden is credited with the discovery of many high-profile breaches including Adobe Systems, JPMorgan Chase, Yahoo, and many other high-profile breaches. Mr. Holden researches minds and techniques of cyber criminals and helps our society to build better defenses against cyber-attacks.
CS3-3: The IIA and ISACA Leadership Session
1:45 PM - 2:45 PM
NASBA Field: Personal Development
Learning Level: Beginner

Anthony Pugliese, CPA, CGMA, CITP
President and CEO
The Institute of Internal Auditors

David Samuelson
Chief Executive Officer
ISACA

Join leaders from ISACA and The IIA as they discuss the strategic transformations both organizations are undergoing to prepare their members and certified professionals for rapidly changing fields. Anthony Pugliese, CGMA, CITP, president and CEO of The IIA, and David Samuelson, Chief Executive Officer at ISACA, will share insights on the future of professional organizations: new approaches to education, the power of community to support professionals’ career paths, and how to prepare for rapid changes – both those that can be foreseen and those that come out of nowhere.

David Samuelson, CEO of ISACA, is a seasoned executive with particular strength in strategic and technology leadership, communications and execution. He has a deep foundational expertise in operational execution, product management and leadership, and deep industry experience in global education technology, software development, consumer publishing, television, and theater. Samuelson has had proven success in both creative ideation and tactical execution of ideas, with an excellent track record of working effectively across global, complex and matrixed organizations. His 25 years in education began at the Minnesota Educational Computing Corporation as vice president and executive producer. He worked at Pearson, the leading global education company, for 15 years in a variety of executive roles, including president of global schools, chief marketing officer and product strategist for Pearson’s US School division, and VP of the Family Education Network. Samuelson’s earlier career in theatre and television included an Emmy award-winning children’s television producer.

Anthony J. Pugliese is president and CEO of The Institute of Internal Auditors (IIA), the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Over a career spanning more than 30 years, Pugliese has been a strategic, hands-on leader, directed strategic expansions into major global markets, pioneered innovative educational initiatives aimed at enhancing members’ professional growth, overseen the internal audit function of a major organization, and defined cultural norms toward greater diversity, equity, and inclusiveness (DE&I).

As CEO of The IIA, he drives the vision and management of a nearly 80-year-old organization with more than 200,000 members, 156 chapters, and 112 affiliates in nearly 200 countries and territories. His focus is on enhancing membership services, creating new approaches to learning and competency development programs, fulfilling The IIA’s multimillion-
A seasoned executive and skilled association strategist with a passion for innovation and technological advancement, Pugliese most recently was President and CEO of the California Society of CPAs, the largest state CPA organization in the United States, with more than 45,000 members. From 1997 through 2018, he served in key leadership positions at what is now the Association of International Certified Professional Accountants, the world’s largest accounting professional organization. His roles included executive vice president of membership, technology, and learning; chief operating officer and senior vice president of the American Institute of Certified Public Accountants, where he oversaw the AICPA’s $50 million relocation to North Carolina; and vice president of business reporting and member innovation.

Pugliese advocates a culture that promotes innovation, collaboration, empowerment, diversity, and achievement. In 2020, Pugliese led development of a Diversity, Equity and Inclusion Committee at CalCPA to identify and address racial and other inequities in the accounting profession. That effort led to development of a groundbreaking study, in collaboration with the Institute of Management Accountants (IMA), to examine race and ethnicity, gender, and LGBTQIA (lesbian, gay, bisexual, transgender, queer, intersex and asexual) orientation in the U.S. accounting profession. Pugliese is long active in the community, from mentoring students to leading business partnerships, such as chambers of commerce.

A graduate of the University of North Florida (Jacksonville), Pugliese has been repeatedly recognized as one of the most influential people in accounting, appearing most recently on the cover of Accounting Today. He holds the AICPA’s Chartered Global Management Accountant (CGMA) and Certified Information Technology Professional (CITP) credentials, and is licensed as a CPA in California, Georgia, and North Carolina.
Gender equity and equality in the technology profession isn’t a new issue, and previous efforts to close the gap haven’t been met with the same success in which they were initially touted. Following a year in which we saw the examination of cultural and gender norms reach new heights, there is a role all of us can play to help level the playing field between men and women in technology.

In this session, participants will learn:

- Gain a better understanding for the true gender disparity in the technology profession that continues well into the 21st century through discussion of recent research, previous studies, and current data.
- Communicate the benefits and challenges of utilizing and implementing blockchain technology.
- Understand what mechanisms have been employed to date to narrow the gender gap in the technology profession and why more action and additional methods are needed - this will be done through overviews of real-life examples employed by organizations today.
- Understand the role that they can play in addressing the gender gap in the technology profession and actions they can take or behaviors they can model to address change on a personal or local level.

Courtney Wilgucki is a Senior Manager in Internal Audit at Vanguard, one of the world’s largest investment companies with approximately $7.2 trillion in global assets under management. She oversees the execution of integrated business audits with a focus on information technology. With 15 years’ experience in auditing and compliance, both externally with Big Four accounting firm EY and internally with organizations such as SunGard and Aramark, she leverages industry and technical expertise to assist in assessing and addressing IT-based risks and controls across business groups around the enterprise. With international experience throughout her career, she has conducted risk-based assurance and advisory engagements on four continents and continues to focus on improving technology risk and compliance management. Courtney holds a number of certifications and designations including the CIA, CFE, CISA, ITIL Foundations, and AWS Practitioner. She also currently serves as Vice President of the Board of Directors for the Brandywine Ballet Company.
Many projects are nowadays delivered through agile or hybrid methodologies. Many of audit’s best practices are aligned with traditional waterfall approaches. This presentation will offer new perspectives around effective control and risk areas that require additional focus to ensure effective project audits. Also, it will offer practical tools not only to conduct audits but also to communicate with practitioners and sponsors well verse on these practices.

After completing this session, the participant will be able to:

- Learn the principles behind agile and hybrid methodologies used in modern projects.
- Map audits’ best practices, specifically in control and risk areas, to agile and hybrid practices to enable effective audit plans and value-added recommendations.
- Learn how to apply tools to plan and execute audits, and use tools to effectively communicate with project practitioners and sponsors who have embraced agile and hybrid methodologies.

Ivan Rincon is an IT professional with 30 years of experience in this area. Ivan is a recognized speaker, having presented in nine PMI Global Congresses since 2006, as well as several ISACA events. In addition, Ivan is a University instructor, teaching project management courses at the Graduate Level in two Universities in Colombia and one in Canada. He moved to Canada from Colombia in 2004 after working in big multinational companies like IBM and HP. He is currently the Director Application Management Services, Ministry of Transportation and Infrastructure in British Columbia (Canada).
CS4-2: The Future of Cyber Risk Quantification and How it is Trending
3:00 PM - 4:15 PM
NASBA Field: Information Technology
Learning Level: Advanced

Gavin Grounds, CDPSE
Executive Director, Cyber Security Strategy and Information Risk Management
Verizon

In almost all areas of business and corporate management, we speak in terms of facts and figures and real fiscal currencies. That is until we start to talk about Cyber Security and Information Risk, where we almost immediately talk in terms of gradients (low, medium, high, critical) and colors (Green, Amber, Red.) This session highlights the challenges of quantification of cyber and information risk, yet providing an actionable roadmap to quantify risk effectively.

After completing this session, the participant will be able to:

• Understand the pros and cons of qualitative risk management, versus quantitative risk management and in particular, why the qualitative methods of measuring and managing Cyber Security / Information domain risks fall woefully short of meeting business needs, to measure and manage cyber security and information risk issues in fiscal terms.
• Learn why the quantification of Cyber Security and Information Risk Management, even when it is being quantified in fiscal terms, needs to go far beyond simply managing to an ALE (Annualized Loss Expectancy) objective. If a company expects its Cyber Security and Information Risk Management functions to be truly enablers of the business, then focusing exclusively on risk reduction - however it is measured and managed - will not meet the need.
• How to scale quantitative cyber security risk and information risk management methodologies, including automation, from a small/medium sized business, to the scale of a Fortune-20, such as Verizon.
• How to capitalize on and maximize the value of insights and information that they already have at their disposal, to effectively manage Cyber Security Risk and Information Risk and in business-relevant, quantitative fashion. The speaker will explain how to adopt his mantra of "Start with what you do know; Improve based on what you could know; Aspire to what you should know"... to get some early returns and wins in establishing and operationalizing a quantification-based risk management framework and methodology.

Gavin Grounds leads Cyber Security Strategy and Enterprise Information Risk Management, as part of the executive leadership team of Verizon’s Corporate Information Security organization. In leadership of cyber security strategy and transformation and delivery of Enterprise Information Risk Management, Gavin drives the development and execution of the cyber security strategy across the Verizon Corporation. Additionally, he leads the Enterprise Information Risk Management function and strategy, covering information & cyber risk, policy, standards, governance and compliance management practices, to ensure that Verizon’s information assets are adequately protected throughout the full system lifecycle and ensuring that operations and controls meet Verizon’s policy, legal, regulatory and governance requirements.
Prior to joining Verizon’s leadership team in 2018, Gavin was Sr. Director of Information Security, Risk & Compliance (CISO, Global Delivery) at DXC in its Global Delivery Organization. Gavin led end-to-end security operations and information risk and compliance management in the delivery of DXC’s broad portfolio of services. His leadership included defining and executing the DXC BionixTM automation strategy for Security, Risk & Compliance on the transformative “Platform DXC.”

DXC was formed in 2017 when Hewlett Packard Enterprise (HPE) spun out its Enterprise Services business and combined it with Computer Sciences Corp. (CSC). At HPE, Gavin served as Global Director of Information Risk Management, Enterprise Security Services, where he led a global organization of more than 1,800 security and compliance professionals to underpin HPE’s services with solid Security and Compliance operations and frameworks and drive significant revenue growth by driving strategic direction for clients through C-Level advisory engagement. In partnership with the Legal department, Gavin served as the primary interface with strategic global clients and with various external agencies and government entities around the globe.

Gavin first joined Enterprise Services (at EDS) in 2000 and has previously held several leadership roles including Director of Global Strategies for Information Assurance and as Client Security Officer for some of the world’s largest Financial, Energy and manufacturing companies.

Gavin has held various leadership roles including CIO of a Business Process Outsourcing company, CEO & Founder of a security consulting firm, security & network strategy leadership for a large off-shore bank and Founder of an industrial plant operations software house.

Gavin is a qualified member of the Institute of Directors, a Chartered Engineer, a Chartered IT Professional and a Certified Information Systems Security Professional. He serves on the advisory board of security technology companies, is a member of the IoT European Council, and as a Fellow of BCS, the Chartered Institute for IT, he is currently the Chairman of the USA Section.

Gavin is the author of several International and US patents and patent-pending applications.
In a world of privacy concerns, customers demand greater assurance for their personal data. How can your organization provide assurance while effectively managing requirement volume and complexity? The surge in cyber requirements necessitates the maturity of two key components: standardization of assurance work, and automation of control and requirements testing. This session empowers participants to establish techniques for building cohesive assurance services, continuous automated testing programs, and strong value narratives while satisfying increasingly complex requirements.

Christie Gross is an innovative and dynamic risk management and cyber assurance professional, recognized for her ability to strategize, implement, and mature comprehensive risk management programs. By developing holistic risk programs that align with corporate objectives, customer requirements, and the constantly evolving technology landscape, Christie builds strong risk narratives and instills confidence in organizational stakeholders. She specializes in developing and delivering new risk management and continuous effectiveness monitoring approaches that identify key and emerging risks and evaluate alignment with risk strategy and appetite.

As an adjunct faculty member at the University of New Mexico, she inspires the next generation of risk and assurance professionals, providing hands-on, use-case oriented instruction around cyber risk management and information security policies.
It can be challenging for many auditors to work effectively with cybersecurity and especially when working remotely or with a virtual CISO. As auditors, what are the best ways to work with CISOs? How do you engage them in the audit without generating an abundance of billable hours? In this session, you will learn about CIO, CSO and CISO roles, and how to collaborate with them in determining and solving security.

After completing this session, the participant will be able to:

- Understand CISOs and vCISO’s roles and responsibilities in multiple organizational types, sizes and sectors
- Organize techniques for managing complex organizational relationships between often divergent roles.
- Evaluate time and cost-effective methods for collaborating across IT, cybersecurity and audit functions.
- Compose audit plans to best leverage CISO’s and vCISO’s time, expertise and resources. Apply ways for efficiently managing audits in collaboration with a CISO / vCISO.

Ron Woerner, CISM is a noted consultant, speaker and writer in the security industry. Ron established the Cybersecurity Studies program at Bellevue University, an NSA Center of Excellence where he still teaches. He has been a featured speaker for TED, (ISC)2, ISACA, and RSA conferences and numerous industry podcasts and webinars. As President and Chief Security Evangelist at Cyber-AAA (https://www.cyber-aaa.com/), he works as a Security Consultant delivering awareness, performing security risk assessments and advising small, medium, and large organizations. His crowning achievement was being selected as the Air Force Association CyberPatriot Mentor of the Year in 2014 for his work coaching High School Students in cybersecurity. Ron has numerous technology degrees and is passionate about building the next generation of cyber professionals.
There is a long and not yet completely understood process to translate data into actionable information, and to create value from data. This presentation discusses some of the basic principles of this process, from understanding how data is perceived within an organization, how the data curation process is organized, how generated value of data is measured and reported, and how relevant information is delivered to the business – all from an auditor’s perspective.

**After completing this session, the participant will be able to:**

- Assess how data is perceived within an organization. From regarding data as a necessary evil to mastering data in a disruptive way, there is a broad range. Learn how to audit data perception by following an online survey within the audience and by discussing its results.
- Audit the Data Curation Process. Analyze and describe the processes and tools in place to monitor and control the compliant use of data and data corrections. Again, from correcting the data upon analysis in a BI system to availability of a data quality dashboard with all relevant aspects of the data, and with automated monitoring of data quality progresses, may different flavors exist. How mature is your organization in this process?
- Measure the generated value of data to your company. Are there any KPI defined and agreed upon on a wide basis? To which degree are information assets based on aligned definitions? How long does it take until a new insight is translated into action? Is this process comprehensive, verifiable and auditable?
- Generate and Deliver Relevant and Timely Information to the Business. In modern systems, BI and operations are not any longer strictly separated. A Hybrid Transactional Analytics Platform (HTAP) helps to minimize time to market for new data and new insights. Hear about these technology enhancements and learn from some real business experiences.
Thomas Baumann is a Computer scientist by training, data scientist by practice, query tuner by spirit. Currently, his position is Data Evangelist at Swiss Mobiliar in Berne, Switzerland. When he is not in his office, trying to get the most out of databases, he is somewhere lecturing on database optimization or database risk management. Thomas holds a master degree in computer sciences from ETH Zurich and is certified as CISA and CRISC. He has been a speaker at different CACS conferences in Europe and North America.

CS5-2: Risk-Based Strategy for “Killer” Hunting Programs
4:30 PM - 5:30 PM
NASBA Field: Auditing
Learning Level: Intermediate

Paul Caiazzo
SVP, Security & Compliance
Avertium

In this session, participants will learn to build a forward-looking threat-hunting program around NIST CSF and the Enterprise ATT&CK Framework. This framework has been successfully applied to over one million devices. Participants will also explore case studies from real-world program implementations representing various business sizes.

After completing this session, the participant will be able to:

- Learn about the use of heatmaps to identify threats against risks.
- Learn how to develop hypotheses and hunt against them.
- Learn how to implement proven hypotheses to bulk up your security posture for future threats.

Paul Caiazzo, Avertium's senior vice president of Security and Compliance, oversees technology alliances and strategic initiatives, guiding Avertium clients through challenging security problems. He also leads Avertium’s internal security and compliance initiatives working to reduce risk across the organization. Previously, Paul was co-founder and CEO of TruShield Security Solutions, one of the fastest growing companies in the cybersecurity industry, and one of three companies acquired by Sunstone Partners to forge Avertium. With more than two decades of experience, Paul has supported the Federal government’s cybersecurity needs in a variety of Department of Defense and civilian agency programs across a spectrum of critical missions. Paul is cybersecurity advisor to the Science and Technology Policy Center for Development, helping the nonprofit organization advance ICT in developing countries. Paul is a certified information system security professional (CISSP), a certified information systems auditor (CISA) and a certified ethical hacker (CEH).
The global pandemic and impacts stemming from COVID-19 shook up business operations across the globe. In this session, we’ll highlight what aspects of secure work anywhere have been successfully in place prior to regional waves of quarantine, supporting productivity through employee mental and physical health considerations, privacy considerations for employees’ personal environments, empowering your plan with innovative solutions.

**After this session you will:**

- Learn what disciplines and business structures have already been operating by “secure work anywhere” standards
- Understand the extent in which internal governance policies help or inhibit employee’s ability to execute their job effectively.
- Hear key considerations to balance security-based monitoring and employee privacy rights within
- Takeaway real-world lessons learned and innovative strategies to keep their “secure-work-anywhere” plans in motion

Todd Fitzgibbon serves as GRC Offering Lead for OneTrust GRC– a purpose-built software designed to operationalize integrated risk management. In his role, Todd is responsible for driving the development and delivery of OneTrust's integrated risk management product as well as driving the refinement of the toolset and offerings. He advises companies throughout their risk management implementations to establish processes to support operations and align with their enterprise objectives, including adopting industry best practices and adhering to requirements relating to relevant standards, frameworks, and laws (e.g. ISO, NIST, SIG and more). Todd works with clients to realize the extent of their risk exposure, helping clients to map their digital infrastructure, assess risks, combat threats, monitor ongoing performance, and document evidence throughout the risk lifecycle.
Building strong relationships with the audit customers is top of mind for most if not all auditors. Whether you are new to the Company or you have a few new audit customers that you would like to get to know better we will share some tactical approaches on how to effectively build and maintain relationships through communication, audit plan execution and talent support.

After completing this session, the participant will be able to:

- Develop and communicate Internal Audit department awareness and brand
- Define a strategy for relationship building and share practical examples of effective implementation
- Tactics for developing an impactful audit plan
- Establish effective communication protocols with audit customers

Yulia Gurman currently serves as Executive Director of Internal Audit and Corporate Security at Packaging Corporation of America (PCA) where she is responsible for Internal Audit, Internal Controls and Corporate Security. Prior to joining PCA, Yulia served as Vice President, Internal Audit at Retail Properties of America, Inc. where she established the Internal Audit function soon after RPAI went public. Yulia also served as Director of Internal Audit at OfficeMax where she managed a team responsible for operational, financial and compliance audits throughout the organization. Yulia attended DePaul University and holds a BS in Accounting/Information Systems. She is a Certified Public Accountant, Certified Internal Auditor, and a member of the Institute of Internal Auditors. She currently serves on the Board of Governors for the IIA’s Chicago Chapter and serves on the Committee of Research and Education Advisors for the IIA. She has previously spoken at multiple IIA International Conferences, IIA General Audit Management, All Stars Conference and the Chicago Chapter Annual Seminar.

Seth Schrank is a Managing Director in Protiviti’s Chicago office. He focuses on delivering solutions to Internal Audit leaders. He has significant experience in assisting clients with internal audit planning and execution, with a specialization in IT audits. He also has extensive experience in scoping and delivering SOX programs for his clients.
Operational resilience is a hot topic these days. The ability to deliver services through operational disruptions is critical—and that starts with identifying essential operations and key risk areas, establishing mitigating controls, and performing scenario analysis and tests to anticipate, prevent, adapt to, and recover from possible failures. Complicating matters, operational resilience efforts must be coordinated between operational risk management, business continuity management, third-party risk management, and other assurance groups.

During this session, participants will learn how to:

- Establish operational resilience governance structure, methodology, and policy.
- Identify critical operations, core business lines, and key risk areas.
- Establish needed controls, set testing cycles, and identify necessary reports.

Knute Ohman is a product manager at Riskonnect, where he oversees the Internal Audit and Compliance product lines. Knute has been in the GRC space for over 15 years acting as a business consultant for GRC products, product manager for GRC products, and a GRC Program manager for a mid-tier bank working with several different GRC products over that time. He has background in process and data analysis, requirements documentation, business case development, client relations, marketing, and program management with expertise in Financial, Governance, Risk, and Compliance (GRC), Integrated Risk Management, and Audit related solutions.

David Brown is a senior product manager at Riskonnect, where he oversees the Enterprise Risk Management and Third-Party Risk Management product lines. His focus is on helping all organizations—from manufacturing to financial—manage their enterprise risks by adopting best practices and leveraging software solutions that improve visibility into their businesses. Prior to joining Riskonnect, David was the product manager for a risk management software provider where he managed the Governance Risk and Compliance (GRC) product line for financial and healthcare customers. David has a degree in economics from the University of North Carolina at Greensboro.
Collin’s dictionary defines “behavior pattern” as "a recurrent way of acting by an individual or group toward a given object or in a given situation." One of the key mechanisms of mitigating risky insider acts is for an organization to both understand and recognize how behavior patterns can impact cyber - and enterprise - security. While your employees are your greatest asset, they are also your largest vulnerability.

This presentation will provide an overview on what the term "insider threat" actually encompasses, from unintentional acts to malicious acts, and everything in between. It will provide details and case studies on fraud, IT sabotage, espionage, trusted third parties, the Critical Pathway, and red flag indicators. The Critical Pathway, as identified by Shaw and Sellers, explains how personal predispositions, stressors, and concerning behaviors can lead up to Insider Threat-like behaviors and/or malicious acts. In addition, this presentation will discuss how one's personal motivations and vulnerabilities can leave their organization vulnerable, how your company's culture can affect insider threat, and how both spies and social engineers work similarly to target you and your employees to gain access to your organization's most sensitive data.

Shawnee Delaney spent nearly a decade with the DIA conducting clandestine Human Intelligence (HUMINT) operations all over the world as a certified Case Officer and one of the few Defense Intelligence Agency (DIA) civilians to be trained at CIA’s iconic training facility. She served as a Supervisory Branch Chief supporting EUCOM, CENTCOM, PACOM and AFRICOM requirements. Shawnee has truly global experience as a human intelligence officer operating in Africa, Asia, Southeast Asia, the Americas, Europe, the Middle East, and the United States. She served in four combat zone tours in Iraq and Afghanistan as a Case Officer and Detachment Chief and worked for the Department of Homeland Security (DHS) where she coordinated and managed intelligence community relationships and partnerships in the protection of U.S. critical infrastructure and industrial control systems for the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

In Shawnee’s ten-plus years in the private sector, she helped create a robust Insider Threat program for a major pharmaceutical company and spent several years building the first Insider Threat program for a prominent Silicon Valley tech company. Shawnee has led complex corporate investigations all over the globe involving fraud, platform abuse, internal data access abuse, counterintelligence, data exfiltration, and attribution of unauthorized disclosures. She holds a M.A. in International Policy Studies with a Specialization in Counter Terrorism and Counter Proliferation, and a M.S. in Cyber Security.
Using third parties can provide a competitive advantage in the global marketplace. However, doing so also increases the risk and exposure to potential violation of Anti-Bribery, Anti-Corruption laws. Effective third-party due diligence is key to mitigating third-party risk and enhancing anti-corruption risk management as an increasing number of ABAC (Anti-Bribery, Anti-Corruption) laws across the globe require organizations to conduct business transparently, honestly, with integrity and to the highest ethical standards.

After completing this session, the participant will be able to:

- Simplify the due diligence process while still obtaining credible results.
- Execute effective due diligence techniques.
- Create an effective due diligence and ongoing monitoring program that is adjustable to different sized organizations.
- Identify common red flags when performing due diligence and be able to better manage third-party relationships through the development of an effective compliance program.
Natasha E. Williams, CFE, CIA, GRCA, GRCP is a #1 International Bestselling Author and a certified professional with over 20 years combined experience in auditing, banking, compliance, risk assessment, fraud examination and accounting. She served nearly half a decade with KPMG LLP working on various consulting and start-up SOX engagements prior to joining Bio-Rad Laboratories in 2005. Her specialty is auditing, compliance, risk management, fraud prevention and detection and overall development of strong internal controls. She manages a global team and has performed and supervised audits in more than 60 countries across the globe throughout Europe, Eastern Europe, Latin America, Africa, the Middle East, China, South East Asia, Australia, Korea, and India to name a few. She has experience consulting small start-ups as well as working with large, matrixed, complex, multi-location and global companies.

CS6-2: How to Mature the IT Risk Management Program in A Growing Company?
10:15 AM - 11:15 AM
NASBA Field: Auditing
Learning Level: Intermediate

Berk Algan, CISA, CGEIT, CRISC
Head of Governance, Risk & Compliance
Silicon Valley Bank

IT Risk Management is simply a tool that helps us weigh options, consider alternatives and make decisions around use of technology. In this session, we will take you through our journey about how we evolved the IT Risk Management framework at a bank from reactive firefighting mode to a proactive process where everyone is involved. We will reveal the best practices we applied and expose the battle scars we overcame along this journey.

After completing this session, the participant will be able to:

- Learn about cornerstones of a mature IT Risk Management Program.
- Understand the challenges associated with maturing the IT Risk Management Program when a company grows.
- Learn about options available to a company to evolve its IT Risk Management Program to adapt to changing times.
- Avoid common pitfalls related to improving an IT Risk Management Program.

Berk Algan is a high-performing Risk Management executive who takes pride in building exceptional Governance, Risk and Compliance (GRC) functions and processes and hiring/coaching/developing an “A” team.

As Head of Governance, Risk & Compliance at Silicon Valley Bank, Berk lead risk management functions for Technology, Security, Business Continuity, Vendor Risk and Project Management processes across global bank locations. He works extensively with federal/state regulators and external/internal auditors and builds relationships with other risk and compliance functions including Enterprise Risk Management, Corporate Compliance, and Internal Audit.
With the recent devastating supply chain attacks, the industry is being forced to completely re-think how we manage risk associated with trusted partners. In this session, you will see a short technical demonstration of just how devastating these attacks are followed by a discussion on how to best manage the associated risk.

After completing this session, the participant will be able to:

- The specifics of how recent supply chain attacks actually happened and learn what the impact is. This will be through them watching the hack live followed by a breakdown of each point of risk in the attack process and suggestions on how to best manage it.
- How to identify hidden risks in the fast-moving world of cyberattacks.
- About the latest difficult to detect malware and other tools.
- Basic countermeasures to minimize risk and exposure to threats introduced by partners and other semi-insider threats.

Keatron Evans is the Managing Partner at KM Cyber Security, LLC, and responsible for global information security consulting business which includes penetration testing, incident response management/consulting, advanced threat hunting services, and cloud security assessments, and training, for the intelligence community, private sector business and academia. Keatron also currently serves as an official advisor/partner to several successful startup firms in the technology sector, and is a course architect and instructor for Ethical Hacking, Threat Hunting and Incident Response for InfoSec Institute. He is also one of the authors of Chained Exploits: Advancing Hacking Attacks from Start to Finish, a book still used by academic and government organizations for teaching hands-on technical security.
There is an old adage that holds that people do what they are motivated to do. And that measurement drives behavior. The vast majority of internal audit professionals are motivated by their mission and by the professional practices framework to deliver value to the organizations they serve. But what is “value” and how do we measure it? And do some of the common measurements we use actually drive the wrong behavior?

After completing this session, the participant will be able to:

- Understand the challenges of measuring value.
- Understand the unintended negative consequences of the metrics most organizations use today.
- Learn a new approach to measuring and tracking value delivery over time.

Patty Miller has significant experience in governance, risk management, and control. She is the owner of PKMiller Risk Consulting, LLC, providing consulting services related to risk management and internal, and assisting internal audit teams with quality assessment and training services.

Prior to founding PKMiller Risk Consulting, she spent 14 years with Deloitte, serving as the lead risk services partner on some of the firm’s most significant technology and consumer business clients. Patty also led the national internal audit risk services practice for Deloitte, consulting with internal audit partners on engagement risk and quality of services. Patty joined Deloitte following a 14-year telecommunications career where she held mid and senior management positions in financial management, billing, internal audit, process design, project and program management, and merger planning and integration.

After leaving Deloitte, Miller served as an executive-in-residence at the University of Nevada in Reno. She is a frequent speaker at locations worldwide and has authored projects for The IIA Research Foundation and articles for the Internal Auditor magazine.

Miller has served in numerous leadership roles with The IIA, including a term as chairman of the global board in 2008 – 2009, as a member of the executive committee for seven years, and as Chair of the Standards Board. She is a recipient of the William G. Bishop III Lifetime Achievement and the Victor Z. Brink awards. She was inducted into the American Hall of Distinguished Audit Practitioners in 2013 and was awarded the Lawrence Sawyer Research Project of the Year Award in 2011. She has served on the audit committee for a public school district and on the board for a nonprofit organization. She was recently recognized as one of the top ten thought leaders for the profession over the last decade.
This session will cover agile concepts and techniques to build a better IT SOX program, deliver faster value to stakeholders, and increase happiness by improving team collaboration and engagement.

After completing this session, the participant will be able to:

- Explore the current challenges and how IT SOX needs to evolve to be effective in today’s remote & virtual environment. (IT SOX today vs. Tomorrow)
- Discuss concepts such time-boxing, collaboration, high-frequency and focused communication, and iterative and adaptive planning and reporting. (Agile Concepts for IT SOX)
- Understand how to leverage agile mentors and servant leaders to implement agile methodologies to IT SOX. (Applying Agile Concepts to IT SOX)
- Learn about different examples of practical application, success stories, and lessons learned. (Case studies from real transformation leaders)

Jimena is an experienced Manager and Agile Coach in Advisory’s Agile Internal Audit practice within Deloitte & Touche LLP. She has 9 years of experience spanning Internal Audit, IT SOX, Business Process Risk and Controls, and SOX Readiness. She has demonstrated proficiency in executing audits consistent with regulatory and industry standards (PCAOB, AICPA, COSO 2013, COBIT, etc.) across the media, technology and consumer products industries.
Jesse Jett is a Senior Manager in Deloitte’s Risk and Financial Advisory group in St. Louis with 12+ years of internal audit and risk advisory experiences across the mining, manufacturing, and financial services industries. In his current role, Jesse helps his clients manage risk by leading global SOX compliance programs and a variety of internal audit efforts. He has experience innovating within Internal Audit and SOX, including the use of automation, analytics, and other tools. He is involved in Deloitte’s CAE Transition and Transformation Labs, SOX Modernization, and other Greenhouse labs. Additionally, he facilitates Deloitte’s ICFR SOX and milestone trainings throughout the firm. He has a passion for all things SOX Modernization – leading change through analytics, automation, collaboration with external audit, assurance by design, and more. He has experience running his own SOX program through modernization initiatives, including an Agile transformation and is passionate about helping clients think about ways to transform their SOX programs and develop better, faster, happier teams. Jesse graduated with an accounting degree from Westminster College in Missouri. He is a Certified Public Accountant (CPA) in Missouri.

**CS7-2: Managing SoD Risks in D365 Through a Comprehensive Access Management Program**

11:30 AM - 12:30 PM  
NASBA Field: Information Technology  
Learning Level: Intermediate

Kevin McCreary, CISA  
Managing Director  
Protiviti

Charlene Lawson  
Senior Manager Internal Audit  
Axon

In this session, participants will learn how to build a strong financial application security program and the components required to manage risk and ensure your program remains successful for many years. They will learn how to start their program with a solid foundation of risk minimized roles and enhance governance processes for a sustainable program that continually manages application security using risk-based concepts.

**After completing this session, the participant will be able to:**

- Learn how Microsoft Dynamics 365 Finance and Operations security is structured within the application and key concepts for grouping key business activities.
- Learn how to develop a Segregation of Duties (SoD) Framework that incorporates risk based concepts that drive decisions on how to address SoD conflicts when they occur.
- How to build a governance program and key processes that need to be established to protect your application from potential fraud or error.
- Learn how to monitor their progress and put key KPI's in place to measure success.
Kevin McCreary is a Managing Director in Protiviti’s Enterprise Applications Solutions (EAS) practice and lead our Microsoft Dynamics ERP services segment. Protiviti is a global business consulting and internal audit firm composed of experts specializing in risk, advisory and transaction services. Kevin has over 15 years of experience helping clients manage their risks and systems of internal control specifically as it relates to ERP and application security risks. I have assisted organizations with their information technology risk management needs.

Charlene Joanna Lawson is a Certified Public Accountant supporting IT Solution Delivery and User Security at Axon Enterprise, Inc (formerly TASER International). In her role, she is responsible for solution design / delivery of ERP initiatives for the global IT organization. Charlene started her career in public accounting at Ernst & Young (EY) in Phoenix, Arizona. She provided consulting and assurance services to a variety of clients in manufacturing, real estate and health care industries. Charlene has held various positions specializing in SEC Reporting and SOX Compliance for manufacturing and SaaS organizations. Most recently, she has been supporting the Axon IT Solution Delivery team as a Functional Analyst designing and delivering solutions for security, warehousing, costing. Charlene has also been an adjunct professor teaching introductory accounting at Chandler Gilbert Community College. Charlene also served as President of the Association of Latino Professionals For America (ALPFA), Phoenix Chapter, where she led a team of leaders from large corporations with a focus of empowering and developing Latino leaders via multiple local and national programs.

CS7-3: Data Driven vs. Ethical Decision Making
11:30 AM - 12:45 PM
NASBA Field: Behavioral Ethics
Learning Level: Intermediate

Mary Breslin, CIA, CFE
President
Verracy

Data empowers organizations to respond in real time, but does “fast” decision making also create problems? This session will explore the value of data and data-driven decision making and examine the pitfalls of decisions made solely using data. A comparison will be made between ethical and data-driven decision making and how organizations can incorporate both. How data can be both unwittingly and willingly manipulated to alter perception and sometimes reality will also be examined.

After completing this session, the participant will be able to:
- Understand the challenges and pitfalls of data-driven decision-making.
- Understand the challenges to ethical decision-making.
- Learn to apply the ethical elements and dimensions to data-driven decision-making.
Mary Breslin founded Verracy in 2014 (formerly Empower Audit Training & Consulting) to provide relevant, insightful, and cutting-edge training as well as internal audit consulting and fraud investigation services. Mary is an internationally recognized speaker and training facilitator. She is a thought leader in fraud, focusing on the role internal audit plays in preventing and detecting fraud in organizations.

Ms. Breslin’s career spans over 25 years in Internal Auditing, Fraud, Accounting, and Management for companies such as Barclays Capital, ConocoPhillips, Costco Wholesale, Jefferson Wells and Boart Longyear. With extensive International experience, she has implemented and managed audit programs in more than 50 countries. She has also conducted major fraud investigations and has been an expert witness in several countries around the world, including a United States Department of Justice (DOJ)/Commerce Department investigation resulting in a $230M guilty plea for a Schlumberger division selling drilling equipment to Iran and Sudan and a $1.6 million criminal fine for Robbins & Myers who facilitated the export fraud on Schlumberger’s behalf.

Prior to Verracy, Ms. Breslin was Vice President and Chief Audit Executive of EZCorp where she transformed a checklist audit function into a trusted advisor audit and fraud detection function which regularly delivered measurable business results through the use of risk-based auditing, data analytics, continuous education and skill development for her leadership team and staff.

Prior to EZCorp, Mary was responsible for developing and implementing the first internal audit function for Boart Longyear, a 120-year-old global mining services company operating in over 40 countries spanning six continents.

Mary was an early adopter of data analytics and has been utilizing analytics in her career in both audit and fraud work for over 15 years. Through her expertise and guidance, she has helped large global organizations leverage analytics to significantly increase coverage, automate continuous auditing and monitoring, and actively fight fraud.

Ms. Breslin attended Rutgers University and University of Phoenix. She has a BS in Accounting and an MBA. She completed her MBA from the University of Phoenix while living abroad after accepting an Ex-pat assignment and moving to Italy. She is a Certified Internal Auditor (CIA) and a Certified Fraud Examiner (CFE). She is a member of the Institute of Internal Auditors (IIA), the Association of Certified Fraud Examiners (ACFE), the American Institute of Certified Public Accountants (AICPA), ISACA, and the Society of Corporate Compliance (SCCE). Ms. Breslin is an instructor and speaks regularly at conferences for the IIA, The ACFE and ISACA.
The internal audit industry is going through immense change, and with this change, most companies are recognizing the need to move faster and shift the way the audit department works within the business. Teams are finding success by adopting an iterative and flexible approach, prioritizing work, and keeping pace with continual changes. This session will explain the benefits of working agile, showcase common challenges to success, and provide practical implementation guidance.

After completing this session, the participant will be able to:

- Learn how to audit with agility.
- Discover why agile auditing is critical to a business.
- Explore best practices and keys to success.

Aaron Wright is the Director of Audit Solutions at AuditBoard, where he works to help audit teams identify and implement purpose-built audit management solutions. Prior to joining AuditBoard, Aaron was an Internal Audit Advisor at Cardinal Health, where he managed a risk-based audit plan and led internal audit projects focused on infrastructure, cybersecurity, and application controls. Additionally, Aaron led the audit technology group where he administered multiple audit software solutions. Prior to becoming an auditor, Aaron was an IT consultant specializing in systems and network administration. Aaron has worked with hundreds of AuditBoard clients as they continue their internal audit digital evolution.

Kelsey Brown is a Senior Director in Walmart Global Audit where she is responsible for Audit Committee and executive reporting, audit methodology, training and recruiting. Kelsey started her career with Walmart as an intern and has been with the company for 13 years. For the first seven years of her career, she supported the implementation of SAP in various capacities in Audit, Finance and Tech. She then transitioned to Global Controllership where she was responsible for supporting the transformation of people, processes, and technology within the Controllership function. She returned to Global Audit in 2020.
Innovation Session 708 Presented by Reciprocity: Operationalizing Governance, Risk and Compliance

12:30 PM – 12:50 PM
Virtual Attendees Only. No CPE Credit

Rob Ellis
Sr. VP of Strategy
Reciprocity Inc.

It’s time to turn GRC on its head and move beyond the outdated “check the box” model of compliance. By definition, to operationalize something means to set something up so that it can be measured. This talk will demonstrate how CISOs and their peers can measure their GRC program against metrics, and use continuous monitoring to mature beyond reactive compliance to take a proactive risk-based approach.

After completing this session, the participant will be able to:

- Measure their GRC program against metrics, and use continuous monitoring to mature beyond reactive compliance to take a proactive risk-based approach
- Use company-wide risks to manage GRC
- Measure the current state of their GRC programs using dashboards and analytics
- Up-level their current GRC programs to a truly operationalized approach

Rob Ellis has more than 15 years of experience leading sales, business development and marketing at SaaS startup companies. At Reciprocity, Rob is responsible for overall revenue growth. One of the company’s first employees, Rob was instrumental in scaling the business from zero - signing up Reciprocity’s first 40 clients, and building the sales and marketing organizations. A startup veteran, Rob has founded companies, and worked in venture-backed startups in a variety of roles including Director of Product at Veetle Inc.; Founder and VP, Product at NotchUp; and Director, Business Operations and Strategic Planning at Peerflix. Rob graduated from Cornell University with a BA in Genetics.
Learn what compliance leaders at some of the world’s most complex organizations are doing to build resilient compliance programs. Focusing their time, effort, and brain power on what’s coming and how they can improve their business. You’d be correct if you guessed they’re implementing new processes and adding new technologies. But the biggest surprise has been around the role people play in this process. Examples of new ideas that people have thought up with increased time on their hands: “It’s not ‘The How’ that holds us back, but rather ‘The Who.’”

Join us for a lesson on resilience and gain a few tips you can apply in your own compliance team.

After completing this session you will be able to:

- What happens to your team when compliance programs falter
- How to focus improvement programs to achieve optimum effectiveness
- How to adapt your compliance strategy to react quickly to changing regulations
- What happens to your team when compliance programs succeed

Jason helps InfoSec, Risk, Internal Audit, Compliance, and IT teams improve their ability to predict, navigate and mitigate against enterprise risk by deploying more efficient workflows and real-time reporting through simple automation. The fruits of his labor have created more than $1.5MM in annual cost savings for the largest logistics company in the world. Classically trained in auditing, Jason spent the first half of his career in internal audit at Swiss Re, TDS, and Arthur Anderson before moving into the technology sector.

Beth has been in the governance, risk, and compliance space for 15 years, helping organizations find technology solutions that solve their biggest challenges. She is extremely well versed in third-party risk management, business continuity planning, and regulatory compliance. When she is not living the GRC-lifestyle, she is applying her technical aptitude and business sense in the Women in Security - Kansas City Chapter (and just recently handed over her reigns as treasurer).
Knowledge Session 805 Presented by ServiceNow: Privacy Management Needs a New Playbook  
12:50 PM - 1:20 PM  
Virtual Attendees Only. ISACA 0.5 CPE Credit

Teresa Law  
Director Product Marketing IRM Products  
ServiceNow

The world’s population produces 2.5 quintillion bytes of data every day. A significant amount of that is personal data gleaned from social media, internet searches, or online purchases. The need to protect this information along with employee and partner information has risen to the top of many organization’s list of strategic initiatives. However, as the scale of the problem continues to grow, current methods for tracking, identifying risks that could lead to the loss or exposure of this data, and responding to these risks aren’t keeping pace. A new approach to privacy management is needed. Join us to discuss the three ways privacy management must change to address the growing data protection problem.

After completing this session, attendees will be able to:

- Discuss the scope of the data protection problem
- Identify 3 areas privacy management must improve
- Suggest 3 changes that can achieve positive results

Teresa is the Director of Product Marketing for the Integrated Risk Management (IRM) products at ServiceNow. Teresa has spent over 20 years in the security and risk industry in various positions including Developer, Product Management, and Product Marketing. Helping businesses recognize and experience the value ServiceNow IRM can provide is her current passion. With a bachelor’s degree in Computer Science and a master’s degree in Business she enjoys the challenge of making technologically advanced products easy to understand.
Privacy rights have been an evolving matter over the last few years and all signs point towards a state-by-state privacy rights act. But how does data privacy affect data security? And how is data privacy different from data security? This session will describe the similarities and differences of data privacy and data security and how both are required to create a mature information security program.

After completing this session, the participant will be able to:

- Define data privacy and data security.
- Determine the similarities and differences between data privacy and data security.
- Identify the trends for data privacy and data security for 2021 and beyond.

Tim holds active CPA, CCSFP, and CISA certifications and licenses. Tim started his path towards running a cyber security and risk advisory firm when he graduated from Miami University in 2015 with a Bachelor of Science in Accounting and a co-major in Business Analytics. Tim has dedicated his entire career to risk advisory services where he provides clients with auditory reports that focus on an organization’s internal controls. Tim specializes in advising businesses on how to leverage their controls to generate efficiencies and maintain compliance with regulatory and audit requirements. As a Manager in the Risk Advisory Services Group, Tim focuses on providing tailored solutions and recommendations to service organizations.
Data analytics is both an art and a science. COVID reporting has indicated total cases, and total deaths. If you are in a very tight community, totals are fine. If you are trying to compare information, then you need another dimension - data normalization. This presentation will show you how data can mislead you unless you are willing to take the time to understand it.

**After completing this session, the participant will be able to:**

- Look at summary data that can mislead you.
- Understand the value of peeling back the summary and understand the data.
- Understand how with COVID reporting, we received truthful reporting, but only part of the picture.
- Learn how taking existing data and using population density would have identified areas of concern early for the COVID pandemic.

John Feigle was the Information Security GRC lead analyst with State Farm Bank for 7 years. His responsibilities include expertise in risk analysis, asset inventory, and control testing. He is currently a member of the State Farm Cyber Security Defense Center with responsibilities for threat response. He has previously worked at Allied Telesis, IBM, and Digital Equipment Corporation, with over 20 years of experience in the security and risk aggregation.

**CS8-3: Automation in the World of Compliance, Governance and Audit - the Future is Here!**

1:45 PM - 2:45 PM  
NASBA Field: Auditing  
Learning Level: Advanced

Vivek Sinha  
Janus Advisory and Consulting Services

Lauren Berrington  
Chief Audit Executive  
Bidvest Advisory Services

In the current landscape we are asked to do more with limited resources and in many cases using a remote workforce. The continuum of Intelligent Automation from basic process automation (RPA) to machine learning and artificial intelligence should be at the forefront of everyone’s mind. Automation can and will revolutionize the way Internal Audit and any other compliance functions execute audits and test controls.

**After completing this session, the participant will be able to:**

- Conceptualize changes that are required to support the requirements of today’s compliance and governance functions.
- Understand how technology and data can be used to drive efficiency and automation of internal audit.
- Understand how they can put together a roadmap for end to end digitalization of their assurance functions.
- Understand that automation can revolutionize the way Internal Audit and any other compliance functions execute audits, test controls, govern and monitor business. It is not merely a pipe dream - the Future is Here!
Vivek is the CEO of Janus Advisory and Consulting Services and a finance professional with over 25 years of international experience in consulting, assurance, shared services, compliance and governance. He specializes in assisting companies with global operating model changes, outsourcing strategies, robotics strategies, and back/ middle office transformations including enterprise transformation, process excellence and process automation. He is widely recognized for his organizational and thought leadership, people and program management and crisis management expertise driving innovation through technology. He has advised several companies across multiple industries with focus on Digital Transformation (Automation) leveraging Robotic & Cognitive Process Automation, Data Analytics and Process Management.

Lauren is the Chief Audit Executive of the Bidvest Group Ltd and has been responsible for the integrated and digital assurance strategies implemented across the 350 legal entities and 135,000 employees in South Africa’s largest conglomerate. She is a founding member of and heads up the ALICE team. Lauren is pioneering the futuristic landscape of IT-related audit services both inside of the Bidvest Group Ltd and beyond. During her 18-year tenure in the audit industry, Lauren worked for the South African, Boston and London offices of PwC before joining the Bidvest Group Ltd in 2012. Lauren holds a BCom(Hons) degree in Accounting Sciences from the University of Pretoria. She is a qualified CA (SA) and CISA. Lauren is the recipient of the PwC Experience Award in 2011 and was a Top-10 Finalist in the SAICA Top 35 Under 35 Competition in 2014.

CS8-4: Hacking Your Cyber Career
1:30 PM - 2:30 PM
NASBA Field: Personal Development
Learning Level: Beginner

Ronald Woerner, CISM
Professor
Bellevue University

Looking to break into cybersecurity or IT Audit or extend your career? To get the right job, consider using hacking techniques to break through the hiring process. Here you’ll learn 3 traits of a well-rounded professional, the career triad, and steps for hacking your career including: visualizing your goals, knowing the best path, social engineering your next boss, and keeping your cyber skills sharp. Cybersecurity jobs are aplenty with basic hacking techniques.

After completing this session, the participant will be able to:
- Implement actionable methods for positioning yourself for a long-term cybersecurity, IT Audit, or GRC career.
- Utilize social engineering, Open Source Intelligence (OSINT), and human hacking techniques and tools to get beyond job descriptions and establish a cyber career.
- Leverage technical and process-based tools for continual active learning to build your experience, certifications and education to land your dream job.
Ron Woerner, CISM is a noted consultant, speaker and writer in the security industry. Ron established the Cybersecurity Studies program at Bellevue University, an NSA Center of Excellence where he still teaches. He has been a featured speaker for TED, (ISC)², ISACA, and RSA conferences and numerous industry podcasts and webinars. As President and Chief Security Evangelist at Cyber-AAA, he works as a Security Consultant delivering awareness, performing security risk assessments and advising small, medium, and large organizations. His crowning achievement was being selected as the Air Force Association CyberPatriot Mentor of the Year in 2014 for his work coaching High School Students in cybersecurity. Ron has numerous technology degrees and is passionate about building the next generation of cyber professionals.

Innovation Session 709 presented by Appsian Security: How Intelligent Automation is Solving Access Governance Challenges in SAP, Oracle, and Beyond
2:35 PM - 2:55 PM
Virtual Attendees Only (No CPE Credit)

David Kantor
Senior Product Evangelist, ProfileTailor GRC
Appsian Security

Managing the governance, risk, and compliance processes is no easy task, especially when considering how complex user permissions can become in ERP applications like SAP and Oracle EBS. Identifying and rectifying SoD violations can be an intimidating project. Redesigning roles often requires long consulting engagements. And audits can be very resource-intensive, both in gathering the right data and in tracking down what’s missing.

In this session, join David Kantor, head of GRC solutions at Appsian Security, as he explores how modern-day technology is being applied to streamline and automate today’s top ERP access governance challenges.

Attendees will learn how to:
- Identify and rectify SoD conflicts in minutes using intelligent automation
- Streamline role design and assignments with risk-aware auto suggestions
- Mitigate the risks of excessive privileges by leveraging user behavior and usage analytics
- Expedite audits with actionable information and minimize the need for manual investigations

David Kantor has been with Xpandion (now Appsian Security) for over 9 years in various roles including support, implementation and customer success management. He now leads the Solutions Engineering & Sales Enablement activities in the company. Previously, Mr. Kantor has worked for several multinational & Fortune 500 companies in engineering and product management roles.
Identity and Access Management (IAM) is critical to protecting sensitive data. However, with issues like password fatigue, siloed directory services, and providing access across multiple devices and platforms, successfully managing IAM is challenging. Decentralized Identity seeks to solve half of the troubled equation.

After completing this session, the participant will be able to:

- Learn what Decentralized Identity is and who some of the key players are in its development.
- Learn some of the benefits that Decentralized Identity is working to provide.
- Be able to compare and contrast Decentralized Identity with current IAM.
- See the current state of Decentralized Identity and some of the current challenges.

Sean is a Managing Director in Protiviti’s Enterprise Applications Solutions (EAS) practice and lead our Microsoft Dynamics ERP services segment. Protiviti is a global business consulting and internal audit firm composed of experts specializing in risk, advisory and transaction services.

Sean has over 15 years of experience helping clients manage their risks and systems of internal control specifically as it relates to ERP and application security risks. I have assisted organizations with their information technology risk management needs.
In this session, participants will learn how to make cyber risk reporting meaningful and actionable across organizational levels.

**The topics covered will be:**
- Risk Appetite as a Foundation for Risk Metrics
- The What, Why and How of Risk Metrics
- Some common challenges in using Metric
- Understanding the Essence of Risk Reporting
- What Makes Risk Reporting Efficient and Effective
- Automation Case Study

**After completing this session, the participant will be able to:**
- Understand the what and why of risk measures / metrics.
- Understand the metric / KRI development process.
- Understand the essence of Risk Reporting.
- Understand what makes Risk Reporting effective.

Priya has 14 years of seasoned experience supporting global organizations with their IT Risk Strategy spanning the areas of Cyber Security, Regulatory Compliance, Privacy and Data Protection. She holds an MBA, is CISSP and is currently a Director in KPMG’s Technology Risk Consulting practice, where she helps build and operationalize Tech Risk programs from ground up or revamping aspects of this in terms of bringing process improvement and automation opportunities.

Priya has authored thought leadership publications featured globally and by multiple press agencies.

She is deeply passionate on Information Security and Women Empowerment / Leadership and as such, has spoken at multiple events – forums, summits / conferences on sharing industry insights, perspective and spreading awareness on these topics.
Everyone is worried about Ransomware now and many are not sure what should be done to prepare for it. This presentation will open with a demonstration of a Ransomware attack, which will only take about 10 minutes. Then follow with a discussion on how to prevent the attacks and how to determine if an organization is ready to respond should they be hit with Ransomware.

After completing this session, the participant will be able to:

- Learn what Ransomware is
- Learn how to defend against Ransomware
- Learn how to assess an organization's risk to successfully being hit by Ransomware
- Learn 10 best practices that will minimize damage that results from being hit by Ransomware

Keatron Evans is the Managing Partner at KM Cyber Security, LLC, https://KMCybersecurity.com, and responsible for global information security consulting business which includes penetration testing, incident response management/consulting, advanced threat hunting services, and cloud security assessments, and training, for the intelligence community, private sector business and academia. Keatron also currently serves as an official advisor/partner to several successful startup firms in the technology sector, and is a course architect and instructor for Ethical Hacking, Threat Hunting and Incident Response for InfoSec Institute. He is also one of the authors of Chained Exploits: Advancing Hacking Attacks from Start to Finish, a book still used by academic and government organizations for teaching hands-on technical security.

As the pace of change continues to accelerate, how we prepare and respond becomes even more important. In this session we will discuss strategies for empowering your team, and yourself, to lead through change and developing the resilience to be ready for the next change opportunity that is coming around the bend.
After completing this session, the participant will be able to:

- Discuss real life examples of how to lead and empower your team to lead through change.
- Share strategies of how to develop and maintain resilience in times of consistent change.
- Discuss when we fail (and we will), how to learn and grow from that failure to prepare for what comes next.

Rachel Tressy, CPA, CIA, CRMA is the Chief Auditor for Voya Financial. She joined Voya in August of 2016 leading the FCR/SOX team, and moved into the Chief Auditor role in August of 2018. Prior to Voya, worked at Cigna for fifteen years, in business and audit related roles. Rachel started her career at Ernst & Young. Rachel has her MBA in Accounting from UCONN and her Bachelors in Political Science from Holy Cross College. Rachel has spoken at numerous conferences including GRC, IIA International Conference and IIA Women in Leadership.

Tuesday | August 10  
4:15 p.m. MDT

Innovation Session 710 presented by Workiva: Empowering Your Audit Department with Analytics
4:15 PM – 4:35 PM
Virtual Attendees Only (No CPE Credit)

Ernest Anunciacion
Director, Product Marketing
Workiva

David Ahonen
Solution Engineer, Integrated Risk
Workiva

Have you ever thought audit analytics sound nice, but you don’t have enough staff? Or time? Or don’t know where to begin without taking on too much? You’re not alone, and the good news is you can start now — without adding any headcount. Start small and gain powerful, fast insight you can build on for years to come. By embedding analytics in every phase of the audit process, internal audit teams can help navigate a remote state of business that’s become more complex, resulting in insights-driven auditing. This is exactly where Workiva can help teams like yours.

In this session, participants will:

- Understand how internal audit can increase investment in audit analytics to facilitate monitoring of key trends and to support continuous auditing.
- Discover how embarking on the analytics journey can help internal audit generate valuable new insights, provide greater assurance, and improve on traditional auditing techniques.
- Get an exclusive product overview and demonstration of Workiva for Audit Analytics.
- Learn how to use Workiva to start on their analytics journey.

Ernest Anunciacion brings more than 15 years of experience in internal audit, risk management, and business advisory consulting to his role as a director of product marketing focused on Workiva’s internal audit solution. A former chief audit executive, he has an extensive background in complex risk and control analysis and process improvement within
the financial services, manufacturing, media, technology, healthcare, and agriculture industries. His expertise also includes ERM and risk advisory consulting.

David Ahonen is a solution engineer at Workiva with a focus on audit, risk, and compliance. He has spent the last five-plus years working with customers in assessing their current state and developing strategic solutions for Sarbanes-Oxley (SOX), audit, enterprise risk management (ERM), and policy management. Prior to Workiva, Ahonen spent five years in public accounting with PwC, working in assurance services.

Tuesday | August 10

CS10-1: Strategies to Scale Security GRC Program in A Multi-Cloud Environment
4:30 PM - 5:30 PM
NASBA Field: Information Technology
Learning Level: Intermediate

Prabhath Karanth, CISA
Director, Security Compliance & Assurance
TripActions

This talk will discuss how to use the different types of control roles - Driver, Subscriber, and Contributor - to implement governance and compliance efforts and how different organizations can use this model for driving their security compliance efforts.

After completing this session, the participant will be able to:

- Streamline security compliance and governance requirements in a multi cloud environment using a centralized control framework that meets different regulatory and compliance obligations including SOC2, PCI, NIST etc.
- Establish formal roles and responsibilities in an organization to drive security compliance and governance at scale.
- Implement centrally managed tooling and automation capabilities that are critical to help drive security compliance and governance efforts at scale across an organization.
- Leverage the established common controls and centrally managed tools together for achieving compliance and regulatory objectives and to increase security posture.
Prabhath Karanth has over 13 years of experience in security assurance, compliance, risk management and governance. He is currently part of the Security and Trust organization at TripActions in a security leadership role as Director, Security Compliance and Assurance. In his current role Prabhath is responsible for driving Security Compliance/Certifications, Customer Trust, Third Party Risk, Business Continuity, Data Governance and Security Awareness & Policy programs at TripActions. Prior to TripActions, Prabhath was a security GRC leader at Adobe where he was responsible for driving security compliance efforts across Adobe’s cloud-based enterprise offerings and strategic security initiatives across Adobe through automation. Prabhath is a Co – author and architect of Adobe common Controls Framework and led the implementation of CCF across all Adobe cloud products, services, platforms and operations. Prior to joining Adobe, Prabhath worked at PwC in their risk assurance practice.

CS10-2 – Anatomy Of 3 Scandals: Why They Occurred and How They Were Preventable
4:40 PM - 5:40 PM
NASBA Field: Auditing
Learning Level: Intermediate

Steven Minsky
CEO
LogicManager, Inc.

Corporate scandals are a regular part of our news cycle and amplified across Social Media platforms by the See-Through-Economy. No matter what type of failure in risk management brought about the scandal, the fact remains that all scandals are 100% knowable ahead of time and 100% preventable. Steven Minsky will evaluate three recent corporate scandals and analyze what could have been done proactively to have prevented them from happening by utilizing sound risk management practices.

After completing this session, the participant will be able to:

- Using the Citibank’s data integration and compliance failures as an example - how sound risk management, data governance, and internal controls could have spared them from paying $400 million to regulators and prevented the immeasurable brand damage suffered as a result of poor internal practices.
- How implementing a strong Third Party Risk Management program will spare them from vulnerabilities, data breaches and - in the event of a breach - protect their brand, revenue and customers by demonstrating, through evidence, that there was a process/program in place. Using the SollarWinds data breach as an example - where hacker's gained access to Solar Winds business environment as a result of a compromise to one of their third party applications, participants will learn how this could have been avoided and how to properly respond if it does happen.
- How to protect themselves from emerging data privacy penalties beyond regulatory punitive damages. As British Airways has seen, class action lawsuits for failure to respect and honor data privacy protections have begun. While many companies didn't take the regulatory requirements or penalties seriously enough to implement strong data privacy programs and governance, the fees associated with lawsuits will get their attention. Laws like GDPR are fair and correct and will only grow in prevalence, business need to learn how to operate within the lines and protect themselves through sound risk management from financial and reputational implications of non-compliance.
Steven Minsky is the CEO of LogicManager and the author of the popular RIMS Risk Maturity Model framework and assessment tool. Steven has presented both strategic and tactical sessions at a variety of conferences, including ISACA’s 2018 & 2019 North America CACS Conference, the IIA’s All Star Conference, the IIA & ISACA’s GRC Conference, American Bankers Association’s Risk Management Conference, the RIMS Annual and ERM Conferences, and the Risk Management Association (RMA)’s GCOR series. He has led educational webinars on a variety of risk-based topics for groups like OCEG, RIMS, PCI&A, and hosted board-level training sessions for many LogicManager customers. Steven is also a patent author of risk and process management technology and holds MBA and MA degrees from the University of Pennsylvania’s Wharton School of Business and The Joseph H. Lauder Institute of International Management.

**CS10-3: Enabling (Zero) Trust in the Identity Workspace**

4:30 PM - 5:30 PM  
NASBA Field: Information Technology  
Learning Level: Intermediate

**William Malik**  
VP of Infrastructure Strategies  
Trend Micro

This session introduces the Identity Workspace, where enterprises exploit digital transformation to strengthen their constituent communities. Enterprises depend on employees, customers, suppliers, partners, and a social and legal context. With face-to-face interactions, these relationships take place naturally. In today’s world, leading enterprises deploy transformative technologies to supplement those lost interactions. These digitally augmented conversations form the identity workspace, which requires trust. Let’s explore whether Zero Trust, paradoxically, can provide trustworthiness?

**After completing this session, the participant will be able to:**

- Understand the value and possibilities of the identity workspace – richer interactions with key constituencies, such as employees, customers, suppliers, business partners, regulators. These interactions will reach far beyond such tools as Zoom, email, web-based order forms, and shared documents. As such, the workspace will introduce additional vulnerabilities, such as risks to trustworthiness and dependencies on reliability. We will look at compensating controls for these risks.
- Explore particular instances of enhanced digital transformation, showing how these enrich the identity workspace beyond conventional digital presence. Examples from manufacturing, education, agriculture, and professional services will show how this enhanced communications medium can enrich corporate culture, strengthen customer engagement, and provide a competitive advantage. Along with the power of these examples, we will address the vulnerabilities they can bring.
- Realize how replacing those absent face-to-face conversations with an identity workspace gives opportunities to reveal a productivity renaissance. Most organizations do not understand the architecture of their social interactions. Deploying the identity workspace requires that architecture be explicit. By clarifying the structure of those interactions, enterprises can apply proven knowledge management principles to optimize the value of their employees’ time and skill.
Find a path towards deploying zero trust to secure their identity workspace. In a safe and trustworthy environment, creativity flourishes and communities grow stronger as they learn and teach together.

William Malik is VP of Infrastructure Strategies at Trend Micro. As a founder of Gartner’s Information Security Strategies service in the mid-1990s, Bill has deep expertise in information security matters. He has spoken internationally on information security, identity management, privacy, business continuity, and enterprise architecture. During his IBM career he guided the mainframe operating system zOS (then MVS) through the process leading to a NIST/NSA B1-level security rating. He taught a graduate class on Information Security Policy at Georgia Tech and authored the chapter “Information Security Policy in the US National Context” for the text “Information Security: Policy, Processes, and Practices,” Detmar Straub, et al., editors. M. E. Sharpe, 2008.

CS10-4: Step Up & Stand Out – Put Your Brand on Display
4:40 PM - 5:40 PM
NASBA Field: Personal Development
Learning Level: Intermediate

Sanjay Patel
Founder
New Tranzitions

Simply put, you represent your own personal brand. In today’s demanding and competitive global economy, people across all industries and functional areas need to understand the criticality of developing and leveraging their personal brand in order to orchestrate and navigate a progressive and successful professional journey. This interactive session explores how you can establish and nurture your personal brand towards the quest for professional development and achievement of organizational goals and objectives.

In this session, participants will:
- Discuss practical concepts to establish your personal brand
- Understand the purpose and value of managing your personal brand
- Examine attributes that define and demonstrate your personal brand
- Explore proven methods for building and further enhancing your reputation and brand credibility

Sanjay has presented to global audiences on topics including personal branding and leadership, reputational integrity, dynamic communication, crisis management, regulatory compliance, project management, and others, and is a frequent speaker at industry events. Sanjay has also spoken at international venues and conducted webinar presentations to audiences around the world. Sanjay’s energetic and engaging personality and skillset have allowed him to successfully collaborate with business professionals at all levels. Sanjay has over 30 years of progressive experience spanning several industries including state government, management consulting, information technology, and financial services. Sanjay’s functional knowledge is also diverse and includes regulatory compliance, strategic marketing, risk/internal controls/audit, strategic sourcing, corporate tax, commercial banking, and graduate level teaching. In 2018, Sanjay self-published an e-book, From Layoff to Take-Off: 31 Practical Concepts to Make a Meaningful Transition after a Layoff, a crafty blend of story-telling with proven self-help concepts.
Innovation Session 711 Presented by MetricStream: Taking GRC to the Frontline to Improve Risk Foresight and Thrive on Emerging Risks
8:00 – 8:20 AM
Virtual Attendees Only (No CPE Credit)

Patricia McParland
Director – Product Marketing
MetricStream

Organizations today face a powerful combination of risks, from mounting regulatory requirements to increasing complexity in vendor ecosystems to sophisticated data breaches and risks from emerging technologies. These risks are interconnected, constantly evolving and must be managed holistically. The first step in strengthening your Risk program is to look at the larger picture and include the entire organization to thrive on risks. In particular, empowering and engaging your frontline employees is key. As the eyes and ears of your organization, they make key risk and compliance decisions every and can protect or expose your organization to various risks.

After completing this session, the participant will be able to:

- Identify current GRC landscape and key trends
- Understand why GRC programs must include the frontline in fighting modern day risks
- Move risk identification to the frontline to capture lurking risks
- Employ AI-powered technology to simplify GRC for frontline to thrive on emerging risks

Pat McParland is Director of Product Marketing at MetricStream. In this role, she is responsible for creating product messaging, product go-to-market plans and analyzing market trends. Pat has more than 25 years of financial data and technology marketing experience and has led product and marketing teams at Dow Jones, Dun & Bradstreet and Honeywell as well as multiple startups. She has a BA from the College of William and Mary and lives in Summit, New Jersey.

General Session 3: Communities and Connection: The Critical Component in your Career
8:30 AM – 9:45 AM
NASBA Learning Field: Personal Development
Learning Level: Intermediate

Lisa Hirtzinger, CIA, CRMA, MBA, M.A.
Senior Vice President, Training & Development
The Institute of Internal Auditors
This is a transformative time: many enterprises and professionals are resetting expectations. While the pace of change may seem overwhelming, there are more opportunities than ever before to engage with other professionals to meet the demands of our stakeholders. Join leaders from ISACA and The IIA, as well as an in-the-field audit practitioner, as they discuss new opportunities and strategies for making connections, finding professional communities, and continuous learning; all of which could be the critical component to your continued success. Both associations are transforming the dynamic ways they can partner with you on your professional journey as you navigate a continuously evolving landscape; especially when it comes to technology risk.

Learning objectives:

- Describe the digital transformations that associations are undergoing to ensure relevant resources and opportunities for business IT professionals
- Explore the future of continuous education and credentials to expand opportunities and keep pace with change
- Discover steps to create a personal learning plan to grow in a role and leverage your global community of peers and colleagues

Lisa Hirtzinger is The IIA’s senior vice president of training and development, focused on developing relevant curriculum and conferences delivered via multiple learning modalities, including in-person, online, facilitator-led, and self-directed, to meet practitioners’ professional development needs. In her 15-year IIA tenure, Hirtzinger has held multiple roles, ensuring high-quality, relevant content is available to support, enable, and assess practitioners worldwide. In her previous role as vice president of professional knowledge and assessment, she was responsible for standards, guidance, and quality services. She also served in director roles in training curriculum, professional guidance, and exam development. Prior to The IIA, Hirtzinger worked in the audit profession at Ernst & Young, LLP and Wells Fargo.

Julia Kanouse is the Chief Membership Officer at ISACA where she is responsible for delivering on ISACA’s overall member and customer experience. Overseeing the membership and marketing functions, her team ensures every step of the member journey is positive and productive. Working closely with ISACA’s 224 chapters around the world, Kanouse leads the strategy on key membership initiatives such as professional development, networking, education and advocacy. Kanouse most recently was the CEO for the Illinois Technology Association (now 1871), which serves the local tech community in Illinois, particularly growth-stage technology companies. Before that, she held several executive roles in membership and marketing at the National Restaurant Association, where she led the development and execution of the National Restaurant Association’s annual marketing strategy, defined new brand architecture, and was responsible for the association’s digital presence.
Membership Business Break: Join The IIA and ISACA to learn more about getting the most out of your membership!
9:45 AM – 10:15 AM

Lisa Hirtzinger, CIA, CRMA, MBA, M.A.
Senior Vice President, Training and Development
The Institute of Internal Auditors

Bob Birdsell, CAE
Senior Membership Manager
ISACA

The IIA 15 min. session
- **IIA Connection** (Why Membership Means More – Local Chapter, Global Network)
- **Member Benefits & Value** (From thought leadership to practical tools that will give you an edge & make you more effective.)
- **Emerge from the Pandemic Better Prepared to Enhance Your Internal Audit Impact** – With the Standards-setting & guidance-producing entity of the internal audit profession.
- Take the next step in advancing your career!
- Q&A

ISACA 15 Minute Session
- **Membership Overview** (Who we are and the community we serve)
- **Benefit Highlights** (Key benefits, Career Centre resources, volunteer opps and chapter engagement)
- **Coming soon!** (Preview of Mentorship program and speak to new engagement opportunities on the horizon)
- Q & A
Closing Keynote Session: Fire Up: Prevent, Break Through, and Extinguish Burnout (and the Power of Resiliency)

10:15 AM – 11:30 AM  
NASBA Learning Field: Personal Development  
Learning Level: Intermediate  

Jessica Rector  
Best-selling author, burnout and mind wellness consultant

Burnout is like a wildfire: spreading quickly and affecting everything in its path. With change, disruption, and uncertainty the new normal, you’re doing more in less time and with less resources. Keynote speaker Jessica Rector leverages her former roles as a TV talk show host and sales leader at a Fortune 100 company to consult companies and train teams to improve engagement, productivity, morale, and health, while reducing burnout and building resiliency. Her Burnout Success Formula offers easy-to-implement, actionable steps to stifle stress and extinguish burnout so you and your team can be more motivated and focused to tackle your obstacles.

Jessica’s vision is simple: Transform Lives. Because her brother died, her mission is to help others truly live. As the top burnout and mind wellness expert, Jessica Rector, MBA is the authority on breaking through burnout and tackling your inner game and turning it into outer success and positive action! As a former TV talk show host and award winning #1 sales performer at a Fortune 100 company, Jessica uses her company’s research to help organizations, leaders, and teams to fire up their thinking and extinguish burnout. Jessica has three college degrees, including an MBA and has written ten books. As a #1 best-selling author, she has shared the stage with Michelle Obama and worked with clients such as Fortune’s #2 “Best Company to work for,” NBCUniversal, and the Dallas Mavericks, and has been seen on ABC, NBC, CBS, and FOX for creating change. When she’s not traveling around the world for work, Jessica spends her time learning about the exciting world of Transformers, so she can carry on real conversations with her eight-year-old son, Blaise, who is a #1 best-seller author and the youngest published author in the United States.
Virtual Workshop: Practicing Agility—A Roadmap Toward Agile Auditing
9:00 AM – 5:00 PM
*Requires a Separate Registration from the GRC Conference*
NASBA Learning Field: Internal Auditing
Learning Field: Intermediate

Shawna Flanders CRISC, CISA, CISM, SSGB, SSBB
Director, IT Training Curriculum
The Institute of Internal Auditors

In an environment where audit risk compounds nearly annually, and budgets continue to stagnate or shrink, internal audit leaders find themselves in a perpetual juggling act, as they try to balance budget, resources, and adequate risk coverage. Conference speakers, articles, whitepapers, and blogs over the last decade have touted the benefits of adding agility into internal audit processes; but, few have provided an adequate roadmap toward agility, let alone provide the stepping stones necessary to begin the journey toward agile auditing.

This one-day workshop is designed to provide internal auditors and audit leaders with their own agility to an agile auditing strategy and an executable plan that will move them from their current state, to a desired future state with improved agility in every phase of the audit engagement.

In this highly interactive workshop, participants will:

- Discover how to assess their current auditing processes in relation to The IIA Internal Audit Competency Framework.
- Explore ways to successfully propose recommendations for adding agility throughout the audit process.
- Understand what agile auditing is and its commonly used terms, and provide a cross-reference between traditional internal audit processes and agile auditing ceremonies and artifacts.
- Discover opportunities where agile and scrum techniques can be introduced into existing internal audit processes as internal auditors begin to explore the value of agile auditing.

Bonus: Rick A. Wright, Jr. The Author of “Agile Auditing: Transforming the Internal Audit Process, Executive Summary” will join us for the last 30 minutes of the session to discuss how he and the subject case study companies began their agile journeys.

A complimentary copy of his book will be provided at the end of the course.
Information is a key resource for all enterprises, and good governance is needed to get the most value from it. COBIT, a world-renowned IT governance framework, helps enterprises develop, organize and implement strategies around information governance and management of IT holistically. This workshop will show how COBIT’s Information Security, Risk and DevOps Focus Areas can be implemented to enhance specific governance practices and activities to specific areas in your organization.

Use COBIT’s Focus Areas to govern and manage information security, risk, or DevOps practices within an enterprise.

Included with registration:
- PDF Download – COBIT Focus Area: Information Security
- PDF Download – COBIT Focus Area: Risk
- PDF Download – COBIT Focus Area: DevOps

As an internationally known governance, risk, and compliance expert in the areas of Cybersecurity, IT Service Management, Assurance and Audit, and IT Controls, Mark’s background spans leadership roles from CIO to Management and IT Consulting in several Federal and State Agencies, Private Firms, and Fortune 500 Companies. With over 25 years of professional experience, Mark has led large IT teams, conducted Service Management and information governance/risk activities for major initiatives, managed enterprise applications implementations, and implemented cybersecurity and governance processes across multiple industries using multiple frameworks including COBIT, ITIL and others. Mark is also a two-time recipient of ISACA’s John Kuyers award for outstanding speaker achievements.