Opening Keynote: Risk Taking and Decision Making in This New Age of Uncertainty

Caspar Berry
Risk-taking and Decision-making Expert

With the coronavirus, all bets are off. As we have seen worldwide in the last decade – among financial and political crises, as well as cultural changes and grassroots movements – it is difficult to make medium-term plans and decisions when we just don't know what's around the corner. With this in mind, former professional poker player Caspar Berry will use the experience gained at the gaming tables of Las Vegas — an overtly and obviously uncertain environment — to bring a new perspective to navigating our own choppy waters.

In this session, participants will:

- Evaluate not only the genuine devastation that COVID-19 has caused, but also the huge implications for the way we live our lives and run our organizations.
- Discover new tools and a different way of thinking about the future to achieve more confidence and increased ROI, whether the near future brings more of the same or something new to the subject of decision-making.
- Gain insights that can serve as a new way to approach what is learned during GRC and in the uncertain times ahead.

Caspar Berry began his working life as an actor in the BBC drama Byker Grove, alongside Anthony McPartlin and Declan Donnelly (Ant and Dec). Then, after studying economics at Cambridge, he made the momentous decision to move to Las Vegas and become a professional poker player. Now a veteran of more than 2,000 speeches in 30 countries, Berry uses these unique experiences to deliver challenging messages about risk-taking and decision-making to maximize returns in an increasingly uncertain world.

Demo: 3 Lines of Defense: Manage Risk, Internal Control, and Internal Audit on One Tool – NOT AVAILABLE FOR CPE

Raashi Bhatnagar
Pre-sales Engineer
MEGA International
Everyday companies face various challenges to efficiently comply with corporate governance including delays due to lack of time, lack of visibility, and poor communication. With MEGA’s HOPEX platform you can cover all three lines of defense (operational management and internal control, risk management and compliance, and internal audit) under one solution. HOPEX will also support you with regulatory compliance while improving operations resulting in improved effective corporate governance.

In this session, participants will:

- Understand how you can achieve effective risk management, internal control, and internal audit while strengthening your corporate governance.
- Learn how you can improve communication, coordination, and collaboration between the 3 lines of defense
- Understand how MEGA’s HOPEX platform allows you to: reuse information for different business purposes, bring visibility to the operation, automate the collection of incidents and deficiencies, and use workflows to ensure timely and clear management.

Raashi Bhatnager is Pre-sales Engineer for MEGA NA, Inc. She has over 10 years of experience working at companies and consulting on their enterprise architecture and governance and risk disciplines. She works with several companies including Gilead, Ford Motor Company, and iA Financial Group helping to ensure their usage of HOPEX is optimized and they can realize effective risk management and corporate governance.

Monday | August 17

CS 1-1: Driving Business Success With Technology Risk Quantification

Luke Nelson
Managing Director, Technology Risk Management
KPMG LLP

Fernando Pinto, CIA
Head of IT Risk
Societe Generale

Technology is vastly improving organizations’ ability to monitor and address their most significant risks. Yet many organizations are hampered by the use of tools that can only provide one-dimensional risk intelligence and metrics of little business value. To become future-ready, organizations need to adopt a risk intelligence view that enables them to improve their risk functions and quantify their risks effectively with a robust, multi-risk perspective.

In this session, participants will:
Identify the various types of risk intelligence tools that may address problems that a business is capable of solving, so their risk functions can help support effective business decision-making.

Understand how organizations can overcome various technology risk challenges by leveraging data analytics, machine learning, AI, and other capabilities now required to stay competitive.

Discuss various international, regional, and domestic regulations that are affecting businesses, and how different types of risk quantification technologies can potentially help in managing them.

Luke Nelson is KPMG’s U.S. service leader for tech risk intelligence, focusing on delivery and innovation capabilities in tech risk quantification, real-time risk reporting, and key risk indicator and metric program design, build, and analytics. He has experience helping clients to identify and assess current state technology risks, as well as working with them to improve their financial, operational, and IT processes and controls, including evaluating their ERM programs. Nelson’s background includes assisting clients in improving resource efficiencies and reducing costs while enhancing their IT product quality and procedural effectiveness. His expertise encompasses using risk-based methodologies and data analysis techniques to evaluate business processes and their system-based controls.

Fernando Pinto joined Societe Generale in September 2018 as an IT risk director and was instrumental in establishing an IT risk framework in the region. He has more than 15 years of risk experience in the financial services industry. Before joining SG, Pinto held various leadership positions at AXA Equitable, including risk director and director of operational risk. Prior to joining the risk division, he was an internal auditor.

CS 1-2: Asymmetric Attacks Mandate Credible Cybersecurity Program

Uday Ali Pabrai, CISSP (ISSAP, ISSMP), Security +, CCSFP
Chief Executive Officer
ecfirst

In this session, participants will:

- Walk through five core areas of a cybersecurity program.
- Review elements of a credible cybersecurity plan.
- Identify key cybersecurity policies.
- Examine seven critical steps for establishing a comprehensive cybersecurity program.

Uday Ali Pabrai is a globally renowned cybersecurity and HITRUST expert, a top-rated dynamic speaker, and the chief executive officer of ecfirst — a compliance and cybersecurity company. His deep expertise encompasses NIST, CMMC, ISO 27001, PCI DSS, GDPR, HITRUST, and HIPAA. His clients include U.S. government agencies, multinational IT firms, and healthcare and financial services organizations. Pabrai has authored several published works. He is a member of the FBI InfraGard, has spoken at their conferences, and served on the HITRUST Assessor Council (2017).

CS 1-3: Exploring Your Risk and Control Career Path
Gregory Haake, CIA, CFSA, CISA  
IT Audit Manager  
MetLife Inc.

Gary Robertson, CIA, CISA, CISM  
IT Audit Manager  
MetLife Inc.

With multiple workforce dynamics, including generational differences, automation, robotics, and artificial intelligence, it is critical to proactively develop and manage your career aspiration goals and milestones. This session will provide insight and tangible career opportunity takeaways for those in risk and control functions (e.g. internal audit, risk management, internal controls, etc.) and interactively explore effective means to expand participant knowledge and visibility to achieve successful career goals.

In this session, participants will:
- Explore potential career paths.
- Identify opportunities to maintain career knowledge and maximize mentorships.
- Manage expectations for career aspirations.

**Greg Haake** has 13 years of experience as an internal auditor. Currently an IT audit manager with MetLife in North Carolina, he previously held various positions with AXA Equitable, Morgan Stanley, Johns Hopkins University, and Blue Cross Blue Shield of North Carolina. Haake brings a unique perspective as an auditor and as an auditee, understanding the different viewpoints of governance, risks, and controls. His internal audit work has included strategic, operational, IT, regulatory, and financial aspects, both domestically and globally, and he’s recruited and actively managed diverse teams. As a frequent speaker, he enjoys sharing his knowledge and training the next generation of internal auditors.

**Gary Robertson** has more than 20 years of internal audit experience in both assurance and information technology roles. He is presently an IT audit manager with MetLife in North Carolina. In previous positions in internal audit functions with public companies, including Altria/Philip Morris, Pall Corporation – a Danaher Company, and Hexcel, Robertson was responsible for recruiting, managing, and developing diverse groups of staff and senior-level internal audit personnel in domestic, international, and global functions based in Zurich, London, and New York. A current member of The IIA Raleigh-Durham Chapter and the ISACA Research Triangle Chapter, he previously held leadership positions with The IIA Westchester-Fairfield Chapter.
Like nearly every other profession in the business world, internal audit and other controls & assurance functions have been forced to cope with the extraordinary environment brought about by COVID-19. Skills, methods and tools that have been advanced and adopting gradually over the past several years suddenly became critical for successful performance. One key area of learning from the pandemic is the importance of making the best possible use of data and digital tools.

Imagine if you could use your transactional data to reveal how processes are actually working and automatically identify instances of deviation from desired processes, control failure, control design deficiency or operational ineffectiveness. Join us as we demonstrate how the Protiviti Controls Assurance app can help you focus on efficiency, automatically identify control failure, and do things right the first time.

**Andrew Struthers-Kennedy** is a managing director, leading Protiviti’s global IT audit practice. He works with clients across industries to deliver outsourced and co-sourced internal audit services, as well as technology and risk management consulting services. Andrew also works with organizations to establish delivery of next-generation internal audit and risk management services through the use of analytics, automation and other emerging tools. He is on the board of his local IIA chapter and is a frequent speaker at IIA and other professional association events.

**Lennart Ebert** became a founding member of Protiviti’s process mining initiative, enabling clients and Protiviti in the use of process mining, both from a technological and business perspective. Lennart was the technical lead to develop the Protiviti Controls Assurance App.
Advancements in information technology and data management platforms enable compliance teams to collect, aggregate, and manage their unstructured and structured data in a single cloud environment, which serves as the single source of truth. Learn how MicroStrategy optimized their Sarbanes-Oxley process, reduced risk, increased control, and enabled insight across the organization. Together, we will share ideas to enhance collaboration in your organization and modernize your audit methodology with connected compliance.

In this session, participants will:

- Identify universal challenges within risk management, audit, and compliance processes.
- Assess best practices for implementing innovative technology to support SOX methodologies.
- Highlight the ways in which partnerships provide value to SOX initiatives.

Ernest Anunciacion is a director of product marketing focused on Workiva’s internal audit solution. As a former chief audit executive, he has more than 15 years of complex risk and control analysis and process improvement experience in the financial services, manufacturing, media, technology, healthcare, and agriculture industries. His expertise combines internal audit, ERM, and risk advisory consulting, and he holds a Black Belt Certification in Six Sigma.

Robert Schmollinger II serves as chief audit executive of MicroStrategy, Inc., and has a record of accomplishment in various industries and multiple financial, control, and risk disciplines. He has led project teams in the integration and implementation of SAP platforms, consolidation of back-office accounting processes, and the achievement of Sarbanes-Oxley compliance. In addition, he has been responsible for establishing collaborative internal audit functions in the life sciences, professional services, insurance, and technology industries. Schmollinger has a deep understanding of business processes, internal controls, and information systems, and he applies this knowledge to make improvements that increase productivity and reduce costs.

Bill Hatcher is a senior manager with Clearview Group and has 12+ years of experience in risk advisory and internal audit solutions. He focuses on helping companies with risk advisory solutions, including implementation and optimization of Sarbanes-Oxley compliance, delivery of outsourced and co-sourced internal audit projects, public company transformation activities, IT governance, and data privacy programs. Based in the Washington D.C. metropolitan market, Hatcher serves in the President-elect role of The IIA–Northern Virginia Chapter.
Business operations, enterprise risk management, and cybersecurity are critical functions that require integration to effectively understand, communicate, and manage risk. These functions are usually isolated organizationally, resulting in uninformed risk and resource decisions that can reduce resiliency and impair efficient execution of mission and business objectives. Organizations must institute organizational tools and behaviors to develop consumable cyber-focused risk intelligence and next-generation resilience methods to respond to the challenges posed by the evolving cyber threat landscape.

In this session, participants will:
- Gain an understanding of the real-life consequences of siloed cyber risk.
- Understand the impact of cyber risk on their ability to achieve business objectives.
- Learn tools and best practices for implementing cyber resilience into their business.
- Enable and promote collaborative discussions across siloed business functions and stakeholders.

**John Eckenrode** is a director at Guidehouse, where he leads the firm’s DoD cyber business. With more than 30 years of experience delivering systems security engineering, cyber security, information technology, and program management support to DOD and civilian clients, he has developed excellent communication and liaison skills with both technical staff and senior leadership. Eckenrode is experienced in designing and implementing complex cyber-enabled systems in a collaborative, team environment with government personnel and contractors. As a champion of cyber resilience, he focuses on providing actionable cyber risk data to decision makers at multiple organizational levels to increase mission resilience and effectiveness while reducing cyber-related organizational risk.

**Ralph Heacock** manages cyber risk and resilience programs for federal clients at Guidehouse. His 10+ year background in cybersecurity and intelligence analysis includes assessing, managing, and mitigating systemic cyber risks and leading cyber threat intelligence for the Global Systemically Important Banks (G-SIBs) of the U.S. financial services sector, U.S.
Geoff Grogan is a manager at Guidehouse, where he helps lead the Department of Defense cyber practice as part of the firm’s Advanced Solutions team. He is a seasoned cybersecurity business leader with more than 16 years of professional experience providing consulting, program management, and risk management expertise to DoD and federal government clients. Grogan’s extensive background in cybersecurity strategy, governance, and policy development encompasses supply chain risk management (SCRM) and non-traditional IT.

**CS 2-3: Making the Three Lines Model Work**

Paul Love, CISA, CISM, CISSP, CIPP  
Chief Information Security and Privacy Officer  
CO-OP Financial

The three lines of defense is a great concept, but how do you make it work? This presentation covers the concept, what works, what doesn’t work, and the value of the model through the eyes of someone who has implemented it from the ground up.

In this session, participants will:

- Understand what the three lines of defense are and how the model brings value to every type and size of organization.
- Gain insights into implementing a thriving three lines of defense model based on the real-world experience of someone who has implemented it from the ground up.
- Be provided with clear next steps on how to communicate the value of the model to key constituent groups and begin implementing a program.

Paul Love is committed to establishing a best-in-class information security (IS) function as CISO at CO-OP Financial. Focusing on budget optimization and integration of cutting-edge techniques and technologies, he builds IS policies, metrics, and programs to deliver on lofty organizational goals. With expertise in strategically orchestrating enterprise wide security efforts and driving coordination with executive leadership and board members, Love fosters continuous business growth while mitigating risk. A thought leader with multiple publications and presentations to his name, he has achieved success with Microsoft, E&Y, and Freddie Mac, solving complex problems in simple, sustainable ways while building IS as a business capability to ensure companies and clients alike enjoy the best possible results. A proud USMC veteran, Love is known for his work ethic and dedication.
Address Emerging Operational Risk and Alleviating Data Blind Spots with AI Powered Risk Management. The digitalization of financial services is in full flight, as financial institutions strive to offer the same levels of service and improved customer experience that consumer markets have enjoyed for some time. This digitalization - providing seamless access to appropriate services on demand - requires great emphasis on client data. This changing digital landscape, and evolving regulations such as global privacy laws, have created a number of factors that contribute to the growing risk ecosystem. In particular, firms find themselves as stewards of new and expanded data sets that are protected by increasingly stringent privacy regulations. As they seek to learn and collect more information about their customers’ activities, behaviours and preferences, financial institutions have had to pivot their practices, policies and strategies to support and protect stakeholders of all kinds, including staff, managers and clients. In this session, we’ll review some of the dynamic elements that pose growing operational and reputational risk, including data sprawl, shadow IT and privacy regulations. We’ll discuss how firms are reacting to the growing threat in terms of improvement of their data structures and governance processes. And we’ll explore how investments and expansion in artificial intelligence can help inform decision making and highlight blind spots to surface issues that may otherwise go unnoticed.

In this session, participants will:

- The importance of data structure and consistency to confidently rely on automation.
- Areas and elements of AI to enhance your risk management program today.
- Considerations for future projects and expansion in AI.

Scott Bridgen serves as a GRC Consulting Director for OneTrust GRC – a purpose-built software designed to operationalize integrated risk management. In his role, Scott 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). Scott 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.

**Knowledge Session: The Role of GRC in Privacy Compliance - 0.5 CPE Available through ISACA Self Claim**

Marshall Toburen  
Risk Strategist, Solutions Marketing  
RSA | A Dell Technologies Company

According to the February 2020 United Nations Conference on Trade and Development, over 75% of countries globally have in place, or are drafting, privacy legislation. In addition, 49 of the 50 U.S. States have at least one privacy-related law (157 State laws in total) and the U.S. Federal government has nine privacy laws in place, although none of the Federal laws are yet as comprehensive as the EU-GDPR.

Many organizations subject to multiple privacy obligations have adopted the best practice to design and operate their privacy programs consistent with the most comprehensive and onerous law to which they are subject. By adopting this best practice, organizations are generally able to demonstrate compliance across all their privacy obligations without operating a separate privacy program for each legal jurisdiction.

In this session, participants will:

- Understand how GRC applies to Privacy Compliance.
- Identify the most important aspect of Privacy Compliance to avoid regulatory fines and sanctions.
- Understand how GRC technology can provide positive assurance of privacy compliance.

Marshall Toburen provides strategic input to the development and marketing of risk-related solutions for RSA and advises customers on risk management best practices. Prior to joining RSA, Marshall served as Director of Enterprise Risk Management for a publicly traded financial services company. In that capacity, Marshall was responsible for the company’s ERM activities, including its ERM practices and technology solutions, information security, insurance risk transfer, loss management, electronic fraud, third party risk management, and Sarbanes-Oxley/ internal controls management. Marshall has previously held positions in the financial services industry, including as Operational Risk Manager, Chief Audit Executive, IT Audit Director, and Assistant Controller.
Knowledge Session: KRIIs for IT Governance in the Post-Pandemic World - 0.5 CPE Available through ISACA Self-Claim

Greg Slayton
Client Partner
Galvanize

The COVID-19 pandemic has forced organizations to adapt to the new realities of remote work, social distancing, and alternative working arrangements. The new policies introduced to govern these situations have stretched the limits of existing technology and operating capabilities—creating increasing exposure to existing and new IT risks. IT risk and assurance professionals must drive an effective and informed IT-risk response. They also need to provide real-time insights into critical IT control areas for business decision-making. This is where quantifiable Key Risk Indicators (KRIs) become very important as they provide early warning signals when risks move in an unfavorable direction.

In this session, participants will:
- Learn why KPIs, KRIs, and KCIs are important in today’s shifting IT risk environment.
- Learn examples of leading, lagging, and current KRIs and what makes them most effective.
- Learn how to establish the right KRIs for IT governance at your organization.
- Learn how InfoSec and Audit teams can collaborate to report on IT risk.

CS 3-1: Leveraging Security for Efficiency in Compliance: Yes, It’s Possible!

Frank Vukovits, CIA, CISA
Director, Strategic Partnerships
Fastpath

Kristal Baird
Director, Accounting Systems
Texas Roadhouse

Maintaining a sound internal control structure is complex; but when done correctly, reduces risk and makes audits more efficient. A key cornerstone that’s sometimes overlooked is security. In this session, we discuss the role of security in
compliance, how to develop a sound approach to security, and where to integrate security into your compliance environment by leveraging industry standards, regulatory frameworks, and real-life examples from companies large and small.

In this session, participants will:

- Discover the best approach to efficiently achieving their compliance goals and how those goals can be audited.
- Hear real-life stories of past implementations and audits.
- Learn how to determine scope and who should be included in the process.

Frank Vukovits has 30 years of experience as an auditor, business software user, and vendor of audit and security software. He has implemented and managed numerous ERP projects and now combines his software and audit knowledge as director of strategic partnerships at Fastpath. Prior to his time working with Microsoft business applications, he was in corporate IT audit for GTE/Verizon for 12 years. Vukovits has presented educational sessions publicly at user groups and audit events for the past two decades. He previously served on Internal Auditor magazine’s editorial board and was an IIA distinguished faculty member.

Kristal Baird leads a team responsible for the security, maintenance, controls, customizations, process efficiencies, and projects related to Texas Roadhouse’s accounting systems, including Microsoft Dynamics AX, Certification, ReconNET, and Hyperion. Her team is also responsible for multiple facets of the period end close process, encompassing income statement analysis, balance sheet reconciliations, accounts receivable, and intercompany. Baird has been with Texas Roadhouse for 17 years in the accounting function.

CS 3-2: Governing Goliath: How to Manage Cyber Risk Against Insurmountable Odds

David King, CISSP, CISA
Founding Member
Cyber Support Alliance

David King walks us through an actual breach case where all reasonable IT controls, including 2-factor authentication, were in place. Yet, cybercriminals still compromised the organization and stole fortunes. This forensic evaluation will provide a unique perspective on how to manage cyber risk against insurmountable odds.

In this session, participants will:

- Gain insight into an actual forensic cybersecurity investigation.
- Learn how to audit business processes as well as IT controls.
- Be better equipped to communicate cybersecurity risk to business leaders.

David King is a trusted advisor for enterprise executives, nonprofits, and small business owners. He specializes in cybersecurity risk management, data breach and ransomware response, and Payment Card Industry (PCI) compliance as
a founding member of Cyber Support Alliance. King is primarily responsible for designing and delivering IT governance, ERM, PCI compliance, and cybersecurity services to businesses of all sizes. He has held civic board memberships with the University of South Florida, Atlanta Public Schools, and the Maynard Jackson Cluster Foundation. King speaks frequently at national and regional events, including ISACA’s Geek Week. He also contributes to national media outlets such as The Wall Street Journal and CNBC.

CS 3-3: Stand Up and Be Noticed: Optimize Your Board Exposure

Joseph Krull
Senior Analyst, Cybersecurity
Aite Group

During the last decade, brand and reputation damage caused by cyber breaches was elevated to the top tier of enterprise risk considerations, and cybersecurity should be regularly addressed at the board level, if it’s not already. This presentation, which draws on interviews and research and includes a case study, advises security and audit executives on ways to initiate or enhance their board interactions to showcase their often-unseen contributions to the organization’s risk-reduction efforts.

In this session, participants will:

- Understand the functions and composition of a Board of Directors.
- Prepare for effective Board interactions.
- Discover how to tailor their messages to be relevant to the Board’s operations and culture.
- Learn how to achieve maximum impact while seeking Board support for major initiatives.

Joseph Krull has provided cyber and privacy consulting to large enterprises on four continents. As a senior analyst at Aite Group, he specializes in cybersecurity, privacy, and IT risk. Previously, at Accenture, Krull focused on cybersecurity’s impact on M&A and cyber/privacy compliance. His prior experience included high-level roles with a Big Four firm and an application security vendor, owner of a business focused on reducing security risk to telecommunications companies, CISO at three Global 1000 companies, and operations officer and military attaché at seven U.S. Embassies. Krull serves on the board of the National Collegiate Cyber Defense Competition and as an advisor to two startups. Multilingual and multicultural, he speaks frequently at international events and contributes regularly to cyber and audit professional organizations in the U.S. and Europe.

Demo Session Break: 3 Steps to Link Your 3rd Party Risk Program to GRC - NOT AVAILABLE FOR CPE

Brenda Ferraro
VP Third Party Risk
Prevalent

Although a critical piece of an overall risk management strategy, traditional GRC programs often lack real-time insights into the risks posed by third parties which can slow down analysis and inhibit decision-making. This session will demonstrate 3 steps to link third-party risk management to GRC tools to accelerate risk identification through the integration of assessments and continuous monitoring.

In this session, participants will:
• Demonstrate 3 steps to link third-party risk management to GRC tools.
• Accelerate risk identification through the integration of assessments and continuous monitoring.

Brenda Ferraro brings several years of first-hand experience addressing the third-party risks associated with corporate vendors, services and data handling companies. In her quest to economize third-party risk, she organized a myriad of stakeholders and devised an approach to manage risk, receiving recognition from regulators and a multitude of Information Security and Analysis Centers (ISACs). In her role with Prevalent, Brenda works with corporations to build single-solution ecosystems that remove the complexities of Third-Party Risk Management by way of a common, simple and affordable platform, framework and governance methodology.

CS 4-1: Configuration of a Common GRC Tool for EHS

Colleen M. Webster
Senior Manager
EY

Kelly Ring
Senior Manager, Risk Transformation
EY

Companies seeking to enhance environmental health and safety (EHS) and corporate social responsibility (CSR) enabling technology are faced with a choice — configure existing GRC technology understood across the organization, select a tool built primarily for managing unique challenges of EHS and CSR, or build a custom solution. All choices serve to help companies manage changing regulatory obligations and risks, streamline workflow, reduce cost of compliance, and influence a culture of proactive compliance.
In this session, participants will:

- Compare and contrast governance, risk, and compliance in the context of EHS and CSR.
- Hear the advantages of the three main enabling technology choices and why this client elected to configure existing GRC technology.
- Discuss why EHS and CSR governance technology is a business imperative, how technology supports process improvement, how process supports technology improvement, and how a GRC tool can help executives better understand risk in their company’s EHS operations and deploy investment more efficiently.
- Examine how a GRC tool enables all three lines of defense to shift their risk approach to from reactive to proactive and calculate the value of engaging the third line of defense to provide an independent perspective on the effectiveness of EHS and CSR risk management, control, and governance processes.

Colleen M. Webster’s Bio Being Finalized

Kelly Ring has more than 10 years of experience at EY across a variety of industries, with early focus on linking technology solutions to business objectives to provide an integrated and holistic view around risk, and most recently emphasizing the maritime transportation industry. She began her career with the firm’s current technology risk practice. She is presently a senior manager in EY’s advisory services practice. As a member of the risk transformation (risk, controls, and technology services) group, she assists clients in analyzing their current technology environments and suggests areas of improvement to minimize risk across the organization while enabling and leveraging ERP and GRC technology solutions in the most optimized and efficient way.

CS 4-2: Control Automation: Reducing Risk and Cost Through Innovation

Ethan Rojhani, CPA, CISSP, CGFM, CFE, PMP
Partner, Controls Advisory
Grant Thornton

Mike Golshanara, PMP, CISM, CRISC
Finance Director, Controls and Compliance
Microsoft Corporation

As business needs and regulatory structures evolve, costs of compliance are increasing. But using traditional approaches, those added costs don’t necessarily bring value to the business. With strategic application of new technologies, companies can reduce risks, create greater efficiencies, and free resources for more sophisticated and strategic value added analysis. Learn how Microsoft has strategically applied new technologies to achieve these benefits and more.

In this session, participants will:

- Explain the business case for investing in new technologies to approach control automation.
- Describe advances in technology and innovation that can be applied to control automation.
Compare characteristics of today’s compliance function with the compliance function in 2025.

Identify three key factors for success in implementing new technologies to approach control automation.

Ethan Rojhani is a partner in Grant Thornton’s business risk services practice. He recently served as national leader for automation of controls, control tests, and risk management using robotic process automation and machine learning tools. Rojhani has led and performed IT audit engagements as well as IT security assessments, including Sarbanes-Oxley (SOX) and Service Organization Control (SOC) 1 and 2. Additionally, he has led the development and implementation of custom tools that integrate cognitive intelligence and analytics to streamline compliance assessment, along with the full lifecycle of compliance, financial, and IT risk assessments and technology assessments.

Mike Golshanara is a finance director (controls and compliance) with operations finance in Microsoft’s corporate finance services. His 12 years with Microsoft include serving as lead for the IT side in the financial compliance group and global compliance lead with operations finance. He manages a large global team with presence in the U.S., Ireland, and Singapore and supports several key organizations within Microsoft. The team focuses primarily on financial reporting compliance (SOX), order-to-cash, and partner incentive and payout, supporting around 10 lines of business accounting for 90% of Microsoft revenue from a SOX perspective. Golshanara previously worked for Deloitte and Touche, Deloitte Consulting, and Siemens. His diverse background encompasses financial, IT, project management, and consulting.

CS 4-3: Batcave to Board Room: Transitioning Geek Speak to Business Communication

Russ Horn, CISA, CISSP, CRISC
President
CoNetrix

Leticia Saiid
Chief of Staff
CoNetrix

Good technology employees can see needs and develop solutions; great ones can transfer this knowledge to others. This presentation will focus on the soft skills required to communicate technical needs to a non-technical audience.

In this session, participants will:

• Understand the science behind presentations and communication.
• Use visual aids, body language, and voice more effectively to enhance verbal communication.
• Discuss tips and tricks to improve written communication.
• Learn ways to grab their listeners’ attention, hold their interest, and conclude strongly.
Russ Horn discovered a passion for technology at an early age, programming and playing on a Commodore 64. Prior to serving as president of CoNetrix, he spent time as a network administrator, systems analyst, university instructor, and IT auditor. His interests also encompass cybersecurity.

Leticia Saiid sees the world in problems, solutions, and equations. At CoNetrix, she served as Tandem Software support manager for several years, building and directing Tandem’s first team of support specialists. Presently, as chief of staff, she focuses on business strategy consulting, serving as a professional coach for company leadership, coordinating corporate projects, and developing employee culture. One of her favorite employee development projects is public speaker training for professionals. Saiid is Security+ certified, has published various security blog posts and articles, has presented multiple conference sessions on information security topics, and was the Silver winner of Cybersecurity Woman of the Year for 2020.

Demo Session: Reduce Risk and Ensure Compliance in the New World of Remote Work with the Intelligent Risk Management Solutions – NOT AVAILABLE FOR CPE

Enrique Saggese
Principal Program Manager
Microsoft

Cath Clark
Senior Attorney
Microsoft

Risk and compliance leaders around the world are now asking themselves, “Is my organization effectively prepared to identify and remediate ever increasing risks?” The COVID-19 pandemic has forced organizations to undertake the rapid digital transformation to be able to remain productive in the new environment. However remote work also brought new types of challenges, such as lack of visibility of employee behaviors, reduced employee awareness of company culture and policies, and increased stressors such as job security or health safety concerns. All these factors can introduce insider risks related to accidental mistakes, as well as heightened risk of some employees participating in malicious types of activities, such as theft of intellectual property. In this session we will demo Microsoft’s intelligent solutions for managing insider risks and explain how they can be effective in mitigating these risks.
CS 5-1: Auditing at the Pace of Change

Jessica A. Clarke, CISA, CICA
Solutions Consultant
Wolters Kluwer

Michael Sekoni, CFE, CFSA, CGMA, CIA, CISA, CPA, CCSFP, AIS, AINS
Vice President and General Auditor
Emergent Holdings/Blue Cross Blue Shield of Michigan Emerging Markets

The world is evolving faster than ever, especially when we consider the impact of technological advancement. The pace of change poses a unique challenge for internal auditors. To meet the challenge, auditors must be agile and always poised to address emerging risks. We also need to lead the charge when working with other assurance teams such as internal control, compliance, risk management, and more.

In this session, participants will:
- Illustrate the importance of addressing emerging risks.
- Formulate an agile combined assurance approach for emerging risks.
- Incorporate a current list of emerging risks into their assessment.

Jessica A. Clarke’s Bio Being Finalized

Michael Sekoni is a seasoned governance, risk, and compliance professional and an executive with 25+ years of experience in auditing, compliance, finance, fraud investigation, and information systems. His expertise spans fraud examination, data analytics, process improvement, internal controls, corporate governance, healthcare, and insurance industries. Sekoni currently directs internal audits and advisory services to ensure Emerging Markets of BCBSM and its operating units efficiently and effectively meet their business objectives. As chief audit executive, he’s responsible for developing and executing a comprehensive audit program for evaluating the company’s GRC activities. Sekoni speaks frequently at national, international, and industry conferences.

CS 5-2: Build Your Very Own Enterprise-class IT GRC Program From Scratch

David Muxfeld, CRISC
First Vice President and Director, IT GRC
Federal Home Loan Bank of Atlanta
An IT governance, risk, and compliance program can be a highly effective mechanism for an organization to manage IT-related risk. However, IT GRC adoption can be challenging, as it is often more art than science. This presentation, part of the speaker’s IT GRC Home Brew series, will establish a recipe for creating a functional IT GRC program from scratch using basic ingredients.

In this session, participants will:

- Describe the basic elements of a functional IT GRC program.
- Apply the methodology for effectively performing independent risk and control analysis.
- Interpret evaluation results to determine control efficacy.
- Understand how to report on risks to enable an organization to make informed decisions.

David Muxfeld is an IT governance, risk, and compliance leader with more than 14 years of experience assessing enterprise risk and information security control mitigations for organizations in the insurance and financial services industries. A pragmatic control practitioner, Muxfeld has successfully designed and implemented various organizational assurance strategies and is a trusted advisor to senior executives regarding enterprise IT risk and control posture. He has held Certified Ethical Hacker (CEH) and Certified Information Privacy Technologist (CIPT) designations.

CS 5-3: The Impact of Risk Maturity on Board Reporting

Angelina Hayes
Senior Manager, Enterprise Risk Management
Nalcor Energy

A risk management function’s ability to deliver a Board-level risk report that meets the needs of Directors is critical. While there are standard visuals and components that are often included, one aspect of risk reporting that is often overlooked is whether or not it is aligned with the risk maturity of the organization. If not, there is a good chance that the report will miss the mark.

In this session, participants will:

- Describe the attributes and competencies that drive risk maturity and consider what a maturity “score” tells us.
- Consider the impact of an organization’s risk management score on its Board-level risk reporting needs.
- Review case studies that provide real-world examples of Board risk reports and templates that met the needs of two organizations with very different risk maturity scores.
- Review a summary of general lessons learned in nearly a decade of delivering risk reporting to Boards.
Angelina Hayes started her career as a risk and control consultant and manager with EY and Grant Thornton, delivering internal audit, internal control certification, risk assessment, regulatory compliance, and other internal control and financial consulting services. Upon joining a global network of internal auditors at Royal and Sun Alliance, she gained invaluable experience in a regulated financial services and mature risk management environment. Hayes then took on the challenge to build a risk management system for Nalcor Energy, a large state-owned utility in Newfoundland, Canada. A longtime IIA volunteer, she held all Chapter Officer positions locally and served a two-year term as the Eastern Canada District Representative, which allowed her to also serve on The IIA Canada Board and The IIA North American Board’s Chapter Relations Subcommittee.

**Tuesday | August 18 | 8:00 – 8:20 a.m. CST**

**Demo Session: Avoiding Audit Pain: How to Automate your ITGCAudit Tasks and Achieve Continuous Compliance** – NOT AVAILABLE FOR CPE

Pawel Jaroszewicz
Senior Engineer
Onapsis

Brian Tremblay
Compliance Practice Leader
Onapsis

Auditing ERP applications, including those run on SAP and Oracle E-Business Suite, has traditionally involved manual processes, limited value tasks, extensive resources, and significant time.

In this session, participants will:

- How to avoid the pain caused by these audits, stay one step ahead of your external auditors and keep your ERP in continuous compliance.
- See how this is all possible while saving your organization's valuable time, money and resources.
- Leave with an understanding on how to receive a complimentary Onapsis Audit Efficiency Assessment that will show you areas of cost savings and automation improvements that can be achieved in preparation for internal and external audits and how to avoid the pain caused by labor intensive manual tasks and audit deficiencies.

**Tuesday | August 18 | 8:30 – 9:45 a.m. CST**

**GS 2: The Neuroscience of Leadership and Performance**
Dr. Jason Jones has spent 20+ years studying human motivation, performance, and workplace engagement. As the author of “28 Days to a Motivated Team,” he understands the challenges leaders face every day to move people to action and inspire people to do their best. Through his keynote presentations and workshops, which utilize the latest in brain and neuroscience research, Dr. Jones teaches people how to activate their natural motivation and become more influential and persuasive. His clients include world-leading brands such as American Airlines, AT&T, Ericsson, Seagate Technology, and the U.S. Postal Service. He has held internal leadership roles with publishing, healthcare, and technology companies.

Demo Session: Data-Driven 3rd Party Risk Management In 2020: Practitioner's Viewpoint – NOT AVAILABLE FOR CPE

Jonathan Ehret
Vice President, Strategy & Risk
RiskRecon

This presentation will discuss some of the challenges faced by third-party risk practitioners, the inherent limitations of a questionnaire-only approach to TPRM as well as a strategy to follow as your mature your own programs. The presentation will also include discussion of how continuous monitoring tools can be utilized to build a more robust picture of the controls actually in place at your third parties.
Jonathan Ehret has been a third-party risk practitioner since 2004. He is co-founder and former president of the Third-Party Risk Association. He has deep experience building and running third-party risk programs in finance and healthcare. He started with RiskRecon in April, 2020.

CS 6-1: Playing With Fire: Pitfalls and Solutions to Vendor Management

Rebecca Rakoski
Managing Partner
XPAN Law Group, LLC

Supplier due diligence is one of the most difficult problems facing business today. In order to comply with newly enacted regulations like the CCPA, GDPR, and NYDFS Part 500, companies must scrutinize their vendors to ensure appropriate safeguards are in place, both contractually and operationally. This presentation will provide an overview of the relevant laws that impact vendor management, and discuss key components of a compliant supplier management program.

In this session, participants will:

- Understand the impact that the CCPA and GDPR has on vendor management.
- Gain insights into creating an effective vendor management program that complies with the pertinent regulations.
- Determine how to operationalize a vendor management program.

Rebecca L. Rakoski is the co-founder and managing partner at XPAN Law Group, a certified Women’s Business Enterprise and Women Owned Small Business. She understands how technology intersects with legal requirements, obligations, and liabilities related to data transfer, as well as cross-border data transfer issues related to international data privacy regulations in the European Union, Asia, South America, and Australia. She can navigate the complexities of different state and federal regulations affecting data transfer, storage, and collection. Rakoski serves on the New Jersey State Bar Association’s Cyber Task Force and also served on a committee that drafted and revised court rules involving electronic discovery in complex litigation matters. She is on the Board of Governors for Temple University Health Systems and is an adjunct professor at Drexel’s Kline School of Law.

CS 6-2: Sink or Swim: Navigating a Metrics Maelstrom

Ben Smith
Field Chief Technology Officer (US)
RSA, a Dell Technologies Business

Are you just starting out on your metrics journey, but don’t know where to dig in amongst the (metric!) ton of books available on this subject? Or perhaps you’ve been metric’ing for some time now, but you still feel that familiar gnaw of “What else should I be thinking about?” Let’s take a look at one aspiring metrician’s bookshelf, where you’ll see highlights and hear stories about why and how each selected book brought value.

In this session, participants will:
- Build out an appropriate curriculum for self-study supporting their metrics program.
- Understand how poorly conceived metrics and measurements can mask operational deficiencies.
- Recognize alternative sources for ideas and insights about risk and security metrics.

Ben Smith is field chief technology officer (US) with RSA, a Dell Technologies business. With 25 years of experience in the information security, networking, and telecommunications industries, he regularly consults on RSA’s security and risk management solutions. His prior employers include UUNET, CSC, and the US Government, along with several technology-oriented startups. He has presented on RSA’s behalf internationally at numerous cybersecurity events sponsored by various organizations and businesses.

CS 6-3: Internal Audit Evolution by Unnatural Selection

Julio Tirado, CIA, CRMA, CISA, CISSP, CFE
Director, Internal Audit
SpiritBank

We are all experiencing changes of all sorts at an ever-increasing rate, and internal auditors can no longer afford to operate with the same mindset or run at the same old pace. Do you want to position yourself as a future-oriented internal auditor? Do you lack a technology background but crave cybersecurity skills? Do you want to be a resource to your organization for tackling emerging risks and trends?

In this session, participants will:
- Review emerging risks and trends.
- Discuss strategies for developing future-oriented competencies and identify modern resources for upgrading their skillset.
- Focus on transforming their professional life to enhance their knowledge, adopt modern skills, and ultimately provide more value to their organization by becoming the internal auditor of the future.

Julio Tirado is the director of internal audit at SpiritBank. He is a member of The IIA, ISACA, ISSA, ACFE, and Infragard professional organizations. Tirado currently volunteers with the Tulsa IIA, ISACA, and ISSA chapters as the facilitator of the Cybersecurity Audit and Risk Roundtable, and serves as the Secretary/Board member of the ISSA chapter.
CS 7-1: Executing Third-party Audit Rights

Natasha E. Williams, CIA, CFE, GRCA, GRCP
Senior Manager
Bio-Rad Laboratories

One of the best ways to provide reasonable assurance that third parties and affiliates are in compliance with laws and regulations and are not participating in illegality is to execute audit rights. This session focuses on incorporating an effective audit rights clause in the contract, overcoming negative reactions to being audited, and getting the business buy-in, as well as how to respond to push-back to get results and what to do when all else fails.

In this session, participants will:

• Gain insights into incorporating an effective audit clause.
• Navigate the auditing discussion to get a cooperative auditee.
• Understand how to obtain business buy-in, how to respond to push-back, and what to do when all else fails.

Natasha E. Williams has 20+ years of experience in auditing, banking, compliance, risk assessment, fraud examination, and accounting. She worked on various consulting and startup SOX engagements at KPMG LLP prior to joining Bio-Rad Laboratories in 2005. Her specialties include auditing, compliance, risk management, fraud prevention and detection, and overall development of strong internal controls. Williams manages a global team and has supervised audits in 60+ countries across Europe, Latin America, Africa, the Middle East, China, and Asia Pacific. She has experience consulting small startups as well as working with large, matrixed, complex, multi-location, and global companies. She joined the Board of Directors of International Center for Reciprocal Training, an educational startup, in 2016.

CS 7-2: Illuminating Dark and Unstructured Data to Comply With Privacy Regulations

Yaniv Avidan
Co-founder and Chief Executive Officer
MinerEye

Although unstructured data makes up about 90% of organizational data, few organizations have succeeded in safeguarding their unstructured data to meet the demands of privacy regulations. This has led to an increased demand for tools that automate data classification and thereby facilitate compliance and data governance. By leveraging
automated tools that leverage artificial intelligence and machine learning, organizations can achieve compliance faster, with less human capital and with higher accuracy.

In this session, participants will:
- Discover how to leverage artificial intelligence and machine learning to comply with privacy regulations.
- Learn about the challenges of unstructured data for privacy regulations.
- Explore automated methods for unstructured data classification.

Yaniv Avidan has more than 15 years of experience in the data analytics domain. He led several business units and corporate innovation teams in business intelligence, machine learning, big data, and cybersecurity analytics. Avidan has led enterprise-class advanced cyber analytics programs at Intel, comprising data scientists and cyber threat intelligence experts reporting to C-level executives. Prior to Intel, he managed an advanced battlefield simulation program for the Israeli Ministry of Defense, partnering with Lockheed Martin and Cubic Defense Systems to develop a complex interdisciplinary system comprised of RT, Comm Relay, and advanced analytics components.

CS 7-3: 28 Days to a Motivated Team: Accelerate Your Team's Engagement and Performance

Jason Jones, Ph.D.
Workplace Psychologist, Author, and Executive Coach

Effective managers and great leaders understand team dynamics and motivation triggers that drive team performance. Attendees will learn the most common motivational triggers of employees, along with 5 scientifically proven factors that drive employee motivation and engagement. Tailored to the needs of the audience, this fast-paced, fun, and practical presentation will share dozens of ideas to inspire each attendee to become a better team member and leader.

In this session, participants will:
- Understand the differences between individual and team motivation.
- Gain tools to assess their team’s current motivation and engagement gaps.
- Develop confidence in their ability to build a high-performing team using practical techniques.

Dr. Jason Jones has spent 20+ years studying human motivation, performance, and workplace engagement. As the author of “28 Days to a Motivated Team,” he understands the challenges leaders face every day to move people to action and inspire people to do their best. Through his keynote presentations and workshops, which utilize the latest in brain and neuroscience research, Dr. Jones teaches people how to activate their natural motivation and become more influential and persuasive. His clients include world-leading brands such as American Airlines, AT&T, Ericsson, Seagate Technology, and the U.S. Postal Service. He has held internal leadership roles with publishing, healthcare, and technology companies.
Organizations need to build for disruption so they can better adapt to the inevitability of change. Join us to hear customer examples and discuss what you can do now to be resilient and how to build a program that provides the agility to respond quickly to disruptions and unexpected risks.

Brandon Reese possesses over 15 years of experience working with Deloitte, Oracle and ServiceNow, in enterprise software sales, management consulting, and information technology consulting. He has successfully consulted with and sold into organizations large and small, from Fortune 500 firms to middle market accounts, across multiple industry verticals. His management consulting experience focused on a variety of areas including systems implementations, risk assessments, operational audits and information technology reviews.

The days of passively managed compliance, risk and management controls are over. Every organization is under intense pressure to maintain a consistent state of compliance in an environment of evolving risk and security controls. All with the need to streamline processes and reduce cost at the same time. You can get ahead of these seemingly opposing forces by putting the latest security and compliance automation tools to work for you.
Join Microsoft and Avanade GRC experts as they walk through a few real world examples of how leading organizations have leveraged technology to streamline audit processes, enable ongoing compliance and reduce costs shifting the GRC function from reactive mode to a highly adaptive, proactive role.

In this session, participants will learn how to:

- Leverage free tools and ones you probably already own to automate many parts of your audit processes.
- Optimize licensing to “right-size” cost and eliminate waste.
- Develop comprehensive dashboards to review and track the state of compliance and security in your environment at any point in time.
- Build a roadmap for the implementation of prioritized security actions.

**Chris Richter** is Avanade’s North America Security Lead. Most recently Chris was CenturyLink’s vice president of global security services, and was responsible for the company’s global managed and professional security services business. Prior to that he served as senior vice president, security services, at Level 3. With over 25 years of experience in IT, Chris has held a number of leadership positions in managed security, IT consulting, and sales with several technology product and services organizations. By helping organizations re-architect their risk management programs and security controls to outsourced, virtualized, and shared-infrastructure services, Chris has assisted numerous IT organizations lower their cybersecurity costs, while improving their overall defense posture. He has acted as both a board member and technical advisor for technology firms, and is a sought-after author and speaker on cybersecurity, risk management, security digital-transformation and IT outsourcing. He most recently contributed to the book “The Digital Big Bang,” published by Wiley & Sons, to be released in September 2019. Chris is also member of the ISSA and ISACA, and holds Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM) certifications.

**Wayne Anderson** is Security and Compliance Architect for Microsoft’s Modern Workplace Center of Excellence, having led global security and compliance, Fortune 500 focused security architecture teams, as well as consulting and managed services architecture capabilities.
Senior Manager  
 Delta Dental of California

The surge of cyber compliance requirements and the demand for risk-based narratives by executives creates the necessity to harmonize regulatory and contractual obligations with data-informed risk assessments. Participants at this session will engage in a thought-leadership approach to the maturation of compliance programs, automated procedural control analysis, and quantitative risk modeling. An example-based approach empowers participants to establish techniques for building a cohesive risk management narrative for leadership while satisfying compliance requirements.

In this session, participants will:
- Identify the relationship between cyber compliance programs, continuous monitoring, and strategic cyber risk management.
- Determine methods for integrating compliance requirements, automated control testing, and quantitative risk analysis processes.
- Cultivate an approach to formulating risk-oriented metrics while satisfying compliance requirements.
- Establish techniques for communicating a cohesive risk management narrative to leadership.

Christie Gross is a risk management and cyber assurance professional with the ability to strategize, implement, and mature comprehensive risk management programs. By developing holistic risk programs aligned with corporate objectives, customer requirements, and the constantly evolving technology landscape, she builds strong risk narratives and instills confidence in organizational stakeholders. Gross 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. Additionally, as a University of New Mexico adjunct faculty member, she provides hands-on, use-case oriented instruction around cyber risk management and information security policies.

David Carter has more than 14 years of experience in cybersecurity and IT compliance. He leads and manages high-performance teams focused on execution, as measured by effectiveness and customer satisfaction in service delivery. He currently manages services concerned with internal cyber risk controls, red teaming, audit support, and technology continuity testing at Delta Dental of California.

**CS 8-2: Shadow IT: The Fight Against a Faceless Enemy**

Mike Skinner, CPA, CISA, CITP  
Partner-in-Charge  
HORNE Cyber

With the cybersecurity threat landscape continually evolving, shadow IT poses a greater risk today than ever before, raising the risk management stakes higher than ever. This session defines shadow IT, identifies shadow IT applications and devices; details why shadow IT poses a critical risk, and discusses best practices to govern it.
In this session, participants will:

- Gain a clear understanding of shadow IT risks today.
- Become familiar with techniques for preventing and identifying shadow IT use.
- Learn about methods to eliminate or prevent shadow IT use by seeking buy-in from end users within company culture.

Mike Skinner was recognized by the AICPA as one of the top technology assurance professionals in the nation under the age of 40. As partner-in-charge at HORNE Cyber, he focuses primarily on enabling clients to fully leverage technology innovations by providing the insights critical to safeguarding their business, customers’ critical data, and brand reputation. He is responsible for information technology audit, regulatory compliance, information security consulting, internal control consulting, and business solution implementation. Previously, Skinner worked for ten years with regional and local firms, including a national retail telecommunications firm and a Fortune 500 international transportation provider.

CS 8-3: Adding Value Around Your Organization’s Digital Transformation Initiatives

Robert Herman
Director, Risk Consulting Robotics, and Intelligent Automation Leader
RSM

Rocco L. Imperatrice, CPA, CFE
Senior Director, Global Internal Audit
Ciena

Amanda Speaks, CPA, CFE
Internal Audit
Ciena

Internal audit is in a unique position to help the organization with digital transformation. Ciena IA is leading by example and helping both the business and IT transform via RPA. This presentation will cover how Ciena started its RPA journey with an opportunities scan to identify use cases within internal audit that were ripe for RPA/automation, and why IA and Ciena decided to implement a citizen developer strategy vs. outsourcing all development tasks to a third party.

In this session, participants will:

- Understand Ciena’s lessons learned, including key considerations and recommendations for other IA organizations wanting to integrate the use of RPA bots to perform manual tasks.
- Gain insights into the selection of RPA software tools and implementation partners.
Discover how IA used their RPA experience to assist the broader organization in starting its broader RPA journey, including consulting around RPA leading practices.

**Robert “Bob” Herman** is a director with 23+ years of experience assessing, designing, and implementing internal control and process improvement solutions. As leader of RSM’s risk consulting robotics and intelligent process automation practice, he helps RSM and clients become more “digital” in assessing and performing internal controls. Trained on various RPA and automation tools and techniques, he has led the design and implementation of 50+ “bots,” primarily in the areas of controls performance and controls validation to help improve and automate repetitive tasks performed by the three lines of defense. Herman has spoken at multiple conferences and training sessions on SAP security and controls, project assurance, and intelligent and robotic process automation.

**Rocco Imperatrice** is a senior director of internal audit at Ciena. He joined Ciena 10 years ago and currently leads the global internal audit function. He previously worked for five years at PwC, auditing high-tech, utilities, oil and gas, and manufacturing companies. His early career background includes more than 13 years of military, private security, and operations experience. Imperatrice served in the U.S. Marine Corps as a noncommissioned officer.

**Amanda Speaks** joined Ciena’s internal audit department in 2016 as a senior auditor. She has since transitioned to a specialist role with responsibility for leading the department’s digital transformation efforts, including initiatives around automation and data analytics. Prior to Ciena, she worked for Stanley Black and Decker. She has 12 years of experience in internal audit and accounting.

**CS 9-1: Endgame: Taking Risk, Security, and Compliance to the Next Level**

Robert Rodriguez  
GRC Manager  
Community Care of North Carolina

Sabrina Hilber, CISA, CIA  
Director, Compliance and IT Assurance  
Community Care of North Carolina

Risk, security, and compliance programs are essential to an organization’s overall success. But how effective can these critical functions be if they are not aligned? Let’s explore the respective roles and responsibilities and demonstrate how ongoing collaboration facilitates the achievement of organizational goals and objectives.
In this session, participants will:

- Understand the importance of intentional overlap of risk, security, and compliance programs.
- Deconstruct the walls that separate risk, security, and compliance.
- Explore methodologies, tools, and techniques to strengthen their organization’s risk, security, and compliance posture.
- Utilize the risk assessment process to measure and improve their compliance and security effectiveness.

Robert Rodriguez has more than 15 years of experience in accounting, internal/external audit, and risk management. He has held a variety of financial and audit positions in the pharmaceutical, retail, insurance, and healthcare industries. As GRC manager at Community Care of North Carolina, Rodriguez is responsible for financial and operational audit, the policy office, and records management, in addition to building and maintaining the ERM framework. A creative problem solver, he specializes in using technology to facilitate training sessions, report results, and design and implement processes.

Sabrina Hilber has approximately 20 years of combined audit and risk management experience in large and small companies within the finance, insurance, and healthcare industries. She takes pride in partnering with management to develop solutions to address challenging risks in the IT and compliance arena. As part of the GRC team at Community Care of North Carolina, she played an important role in developing and implementing the ERM framework.

CS 9-2: The Fine Art of Stepping on the Same Rake

Alex Holden
Chief Information Security Officer
Hold Security, LLC

Hackers are learning from our mistakes and developing more resilient and devastating attacks. Our defenses, while improving, are still making the same mistakes they have for decades. We will discuss several recent breaches as well as lessons learned.

In this session, participants will:

- Understand common techniques from the hackers.
- Build defenses to scale against the most common threats.
- Learn from recent security breaches.
- Take home practical advice for defenses of today and tomorrow.

Alex Holden is the founder and CISO of Hold Security, LLC. Under his leadership, Hold Security has 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, and Yahoo. He researches the minds and techniques of cyber criminals to help our society build better defenses against cyber-attacks.

CS 9-3: Developing Security Empowered People: A Case Study

Susanne Senoff, CISSP, CISM, PMP-ACP, CISA, CIPT
Senior Director
Arm

People are often the greatest source of cybersecurity risk for a company, as 90% of breaches start with a phishing attack, and issues like accidental data loss and insider threats continue to plague security teams. How can you transform people from your greatest cybersecurity liability into an effective frontline defender?

In this session, participants will:
- Walk through how one company approached this transformation and lessons learned to date.
- Discover a framework for improving security empowerment and changing culture, and explore how to apply this framework to their own organization.
- Learn strategies and tools for overcoming cultural resistance and measuring people behavior.

Susanne Senoff is senior director of enterprise security and governance at Arm, where she has led the development of its governance, risk, and compliance function. Prior to Arm, Senoff was a practice director at Accretive Solutions in Northern California’s technology and compliance group, where she worked with startups to multibillion-dollar companies on improving their security posture. Additionally, Senoff held director-level roles in Microsoft’s O365 security group and in Morgan Stanley’s financial and operational risk and compliance functions. She has 20+ years of executive leadership, program management, risk management, cybersecurity, and consulting experience across finance, HR, operations, engineering, and risk functions.

Demo Session: SAY HELLO TO COMPLIANCE BOTS: From Ice Age to Space Age - NOT AVAILABLE FOR CPE

Jason White
Chief Strategy Officer
Neverfail
Continuous Controls is the first RPA BOT toolset that automates evidence collection, control testing, and remediation to provide a SINGLE INTEGRATED TOOLSET that removes the traditional cost, risk, and multi-dimensional complexity of IT audit & compliance.

In this session, participants will:

- Discover how the Continuous Controls Robotic Process Automation (RPA) platform is transforming compliance and risk management.
- Discover how automated evidence collection is removing this burden and costs from internal teams.
- Discover how automated testing is being designed to auditor requirements, while assessing evidence in real-time to ensure continuous control adherence.
- Discover how organizations can automate remediation management for any control test failure.
- Discover how Continuous Controls can enable your GRC tool of choice with RPA BOT capabilities.

Jason White is responsible for architecting and communicating the company’s Continuous Controls value proposition and go-to-market strategy. White brings a wealth of strategic and executive level success from his 19-years with Planview, the global leader in Enterprise Work and Resource Management. At Planview, White held many leadership and executive level positions with the most recent having served as Senior Vice President of Global Solution Consulting. In that role, White led the team responsible for painting the vision for how Planview solutions deliver enterprise-wide value for the most complex organizations in the world.

CS 10-1: Machine Learning Monitoring, Compliance, and Governance

Andrew Clark, CAP, GStat
Chief Technology Officer
Monitaur

With Machine Learning (ML) taking on a more significant role in decision making, ML is becoming a risk management and compliance issue. In light of increasing regulatory scrutiny, companies deploying ML must ensure that they have a robust monitoring and compliance program. This presentation will provide context around relevant regulations, outline critical risks and mitigating controls for ML, and provide an overview of monitoring and governance best practices.

In this session, participants will:

- Understand the need for ML governance and risk management.
- Know — at a high level — the relevant regulations for ML.
- Describe how to construct a ML governance program.
Andrew Clark is a co-founder and chief technology officer of Monitaur, a machine learning assurance company focused on solving a key problem that has been preventing widespread machine learning adoption: the lack of a holistic approach to machine learning risk management. Monitaur’s risk management and regulator-friendly ‘SIEM’ system records all model predictions with an understandable description of why a transaction has occurred. Clark has appeared as a speaker at numerous conferences, presenting on open source audit analytics, machine learning, and emerging technologies.

CS 10-2: Arming the Sentry

Jude Viator, CIA, CISA, CRISC
Associate Consulting Director
P&N

While organizations can invest in stringent logical and physical security protections, the human element of security is paramount for success. This session navigates the concepts of elevating security measures by aligning the parallel human, system, and physical security controls through a deliberate approach of training, culture, and investment. We will discuss real-life examples, as well as best practices and concepts for consideration.

In this session, participants will:
• Describe the components of the security equation, including the human and non-human elements.
• Evaluate the opportunities to enhance and formalize human preparedness to act as a security sentry.
• Associate and expand on content through sharing of real-life examples.

Jude Viator has extensive experience in conducting and managing internal controls based projects, as well as IT/IS security assessments for various organizations, including publicly traded businesses. His background encompasses conducting and managing outsourced/co-sourced internal audit engagements, BSA/AML compliance assessments, operational/compliance audits, IT general controls assessments, internal control assessments, SOC 1/SOC 2 exams, agreed-upon procedures engagements, risk analyses, best practice assessments, and process/function reengineering. Additionally, he has identified and tested SOX 404 IT relevant controls, and conducted all aspects of internal audit engagements, including reviewing internal controls, interviewing client personnel, assessing the possibility of fraudulent activity, developing test procedures, scripting the report, and presenting the report and other matters to client management and oversight committees.

CS 10-3: The Next Generation of Discussions With the Audit Committee

Stephen Leslie, CFA
Vice President, Global Risk, Data, Corporate Functions, and Corporate Development Audit
Internal audit not only must respond to market and business changes before becoming irrelevant, but also be prepared to assess if the business is undertaking its innovation and transformation initiatives in the best possible manner. Audit committees must also ensure they are overseeing the right risks during dynamic change, including outsourcing of many business functions and the need to adapt their oversight responsibilities when there is increasing reliance on internal audit (whether internal or outsourced).

In this session, participants will:

- Understand the challenges faced by internal audit organizations.
- Describe a vision for the next generation of internal audit along with the skills required for the next-generation internal auditor.
- Provide examples of emerging technology changing the audit process.
- Evaluate how audit committees need to adapt their oversight responsibilities.

Stephen Leslie leads the audit function at TD that covers risk management, enterprise data asset risk (including machine learning and artificial intelligence), and corporate functions on a global basis. His experience spans 27 years in commercial banking, credit risk management, retail banking, corporate operations, and audit. He is highly active on various not-for-profit boards, primarily focusing on child and youth development.

Ram Balakrishnan leads Protiviti’s internal audit practice in Canada and has 20+ years of professional experience providing internal and external audit, team building, and executive consulting services. He developed his expertise in technology and operations audit areas through both industry and public practice. His industry background includes positions with a major Canadian workers’ insurance board as the chief audit executive and vice president of internal audit and as the global technology operations internal audit leader at a global technology company, where he helped set up the risk performance and audit team. Balakrishnan also has extensive consulting and audit experience working with the Big Four public accounting firms.

Wednesday | August 19 8:30 – 9:45 a.m. CST

GS 3: Resilience Today and in the Long Term

Moderator: Greg Grocholski, CIA, CISA
We have all been impacted by the COVID-19 pandemic, both in our current roles at our organizations and in our ongoing professional development goals. To support our members, The IIA and ISACA offer several resources to support and guide professionals in this time of change and beyond. Join leadership from the two organizations as they share their members’ stories of not only adding value to their enterprises—ensuring business continuity, mitigating risk and testing operational resilience—during the pandemic, but how they have continued to add competencies and adjusted to a new environment to continue their professional success.

Greg Grocholski is responsible for leading and managing the internal audit department on a global level, to ensure the implementation of internal audit best practices worldwide, as well as to coach the company’s internal audit employees to maximize their contributions to achieving the company’s objectives. Grocholski is internationally respected in the audit field and is affiliated to ISACA, for which he has served in various leadership roles. Prior to SABIC, Grocholski attained an impressive track record in the global chemicals industry with more than 30 years of service at The Dow Chemical Company. He achieved numerous promotions in the audit and finance functions, most recently holding the posts of CAE and global director of business finance.

William Michalisin is the Executive Vice President & Chief Operating Officer for The Institute of Internal Auditors (IIA), the global professional association and standard-setting body for internal auditors. The IIA serves more than 200,000 members in over 200 countries and territories and acts as the internal audit profession’s recognized advocate, educator, and provider of standards, guidance, and certifications globally.

In his current role, Michalisin leads operations and core services offered to IIA members globally, including Membership, Certifications, Training & Conferences, Standards & Guidance and Professional Knowledge, Advocacy & Government Relations, Chapter and Institute Relations, Partnerships, Sales and Business Development.

Prior to joining The IIA, Michalisin was Industry Marketing Leader for Consumer & Industrial Products at Deloitte, which included responsibilities for cross-functional delivery within aerospace and defense, automotive, consumer products, process and industrial products, retail and distribution, and travel, hospitality, and leisure sectors. Earlier in his career,
Michalisin was a consultant delivering business process strategy, risk management and fraud/forensic investigation services at both Deloitte Consulting and Accenture, to clients in multiple industry sectors.

Michalisin graduated magna cum laude from Columbia University with a master’s in Strategic Communications and has a bachelor’s degree in International Relations and Economics from Bucknell University. He also has his CIA designation and is a member of the Institute of Internal Auditors.

Nader Qaimari is chief learning officer for ISACA’s learning and certification offerings for individual professionals, including the Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Control (CRISC), Certified Information Security Manager (CISM), Certified in the Governance of Enterprise IT (CGEIT), and CSX Cybersecurity Practitioner (CSX-P) certifications. He also leads ISACA’s editorial and publishing efforts, including the ISACA Journal. Previously, as group president of Follett School Solutions, Qaimari launched new book fair and digital curriculum businesses while running Follett’s software and service platforms, leading 1,700 associates globally. Prior, after advancing from product management and strategy roles at Cengage, he led sales and marketing across global markets as a senior executive.

Wednesday | August 19

**Demo Session: VaR: Next Generation End-to-End Risk Identification and Quantification - NOT AVAILABLE FOR CPE**

Karl Viertel
CEO
Alyne

In this session, participants will:
- End to end compliance and risk management practices for many various industry standards.
- Placing a value on risk: qualification and quantification of risk.
- Learn about RegTech and it’s benefit to the GRC arena.
- Digitalisation of processes.

Karl Viertel, CEO, is involved in running Alyne’s corporate strategies and sales activities. Prior to Alyne, Karl delivered security, risk management and governance solutions to organisations in Europe, America and Asia Pacific in his role as Director for Deloitte & Touche in Germany and Australia. He started his career delivering complex IT programs to European banks at Accenture.
Closing Keynote: The Future Is Now: Emerging Technologies Are the New Normal

Kimberly Ellison-Taylor, CPA, CGMA, CISA
Global Accounting Strategy Director, Financial Services Group
Oracle

The accelerating pace of change is affecting all facets of an organization. From heightened customer expectations and demographic trends to a changing regulatory environment, organizations of all sizes are implementing emerging technology to innovate and transform. The benefits of emerging technology to improve operational efficiency, digital intelligence, and business influence are key proof points.

In this session, participants will:

- Discuss emerging technologies such as blockchain, artificial intelligence/machine learning, internet of things, and robotic process automation.
- Consider how such technologies are transforming organizations, enabling competitive advantage, and driving greater year-over-year revenue.
- Discover new leadership approaches to inspire and motivate team members.

Kimberly Ellison-Taylor has a background in strategy, finance, people leadership, digital engagement, business development, and technology in the public sector, telecommunications, financial services, healthcare, and technology industries. As global executive director of finance thought leadership at Oracle, she promotes transformation and digital strategies for SaaS, IaaS, and PaaS technologies in organizations of all sizes. Ellison-Taylor previously held leadership roles at Motorola, KPMG, Prince George’s County Government, and NASA Goddard Space Flight Center. She was Chairman of the Board for the American Institute of CPAs, Association of International CPAs, and Maryland Association of CPAs. She was named among the Top 100 Most Influential People in Accounting by Accounting Today and among the Top 25 Most Powerful Women in Accounting by CPA Practice Advisor.