



ISACA[®]

Toronto Chapter

Annual Summer Conference 2024

June 26 - 27, 2024 (In-Person or Virtual)
8:30 am To 5:00 pm EST

Location: EY Tower, 100 Adelaide Street West, 31st Floor, Toronto, ON, M5H 1S3

PROGRAM BROCHURE

Register @

<https://www.gifttool.com/registrar/ShowEventDetails?ID=2200&EID=31749>

to earn up to 12 CPEs

DAY 1: Wednesday June 26, 2024

7:45 – 8:20 AM	Registration and Continental Breakfast	
8:20 – 8:30 AM	Opening/Welcome Remarks Margaret Lee-You, Conference Chair & Najib Hayat, President Toronto Chapter	
8:30 – 9:30 AM	Keynote: The Evolution of Audit Work in the Digital Age Shelley Spence Auditor General of Ontario	
9:30 – 9:45 AM	BREAK / ROOM CHANGE	
	STREAM A	STREAM B
9:45 – 10:45 AM	Reimagining Governance and Oversight Amid Digital Disruption Prashant Masand, Partner, Strategy, Risk & Transactions Aby Mahmoud, Senior Manager, Audit & Assurance Deloitte	So, you receive SOC Reports from your 3rd Parties - Now what? Sameera Jamal, Partner, Matthew T. Batterton, Can SOC Leader, Partner, Bronwyn Kemp, Senior Manager, Technology Assurance EY
10:45 – 11:00 AM	BREAK	
11:00 – 12:00 PM	Navigating the Complexities of Data and Technology Risk in ESG Mark Selvaratnam, Director, Digital Risk Solutions Belal Raifai - Manager, Digital Risk Solutions PWC	Product Security Testing to Combat Supply Chain Attacks Ismael Valenzuela, VP – Threat Research & Intelligence BlackBerry
12:00 - 1 PM	LUNCH	
1:00 – 2PM	Re-inventing Second Line of Defense to Embrace Digital Disruption Eduardo Delgado, VP - 2LoD Information Security Risk Management TD	Demand for Data Governance Programs in the Age of AI Michael Kostanecki, Associate Director, Team Lead; Tarun Dhawan, Associate Director Protiviti
2:00 – 2:15 PM	BREAK	
2:15 – 3:15 PM	Managing Risks in Digital Payments Benjamin Bernal Diaz, Director, Enterprise Data Protection Stephanie Slavik, Director, Governance & Oversight, Enterprise Data Protection Scotiabank	The Impacts of Artificial Intelligence on DevOps Security Miguel Mendez, Generative AI Tech Lead Wissam Bashour, Senior Manager - Cyber Risk Deloitte
3:15 – 3:30 PM	BREAK	
3:30 – 4:30 PM	It's Not Intelligence It's Functionality! Dr. Miklos Vasarhelyi, KPMG Distinguished Professor of AIS Rutgers Business School	Secure Cloud Application Development with Container Orchestration on Google Cloud Platform Sarah Shafey, Delivery Executive, Google Cloud Services, Maulik Thaker, Delivery Executive, Paul Williams, App Modernization Engineer Google Cloud Consulting

Day 1 Keynote Session

8:30 am – 9:30 am

The Evolution of Audit Work in the Digital Age

SESSION DESCRIPTION

Technologies can be disruptors and can propel positive changes in organizations, bringing with them risks that auditors need to assess. IT systems are thoroughly embedded in every aspect of the Ontario public sector: from education and child welfare to medical care, social assistance, the judicial system, and public transportation. The Auditor General of Ontario, Shelley Spence, and also former partner at Deloitte, has a unique vantage point on the risks and benefits of the technologies that house peoples' most personal data and give them access to essential services.

This session explores the IT landscape in the Ontario Public Sector, highlighting the trends and patterns that will be discussed in this conference as well as those the Office of the Auditor General of Ontario has found in recent IT-related audits. It also introduces changes very recently tabled to the Federal Freedom of Information and Protection of Privacy Act and the Province's new framework for the responsible use of AI. The challenges faced by government in our digital age likewise pose challenges for auditing government systems. We need to be aware of the importance of increasing efficiencies and accuracy of financial reporting along with the wise use of artificial intelligence and other technology tools.

As we adopt disruptive emerging technologies, looking at cybersecurity, the impacts of artificial intelligence, transparency in reporting, data governance and oversight, as auditors we need to quantify and measure risk. These are all immensely important issues associated with technology and they are made tangible at conferences such as this one. We can only benefit, as a society, from collaborating and strategizing together with a robust exchange of ideas and knowledge.

KEYNOTE SPEAKER



Shelley Spence
Auditor General of Ontario

Shelley Spence, CPA, CA, LPA

Shelley Spence is Ontario's 14th Auditor General and began her ten-year term of office in January of this year. She brings over thirty years of professional experience in audit, internal control and technology auditing in the public sector. She was most recently Partner with Deloitte LLP, where she spent over six years helping oversee the Canadian Government and Public Service Assurance practice. She has consulted for hundreds of public and private sector clients, with extensive experience at federal, provincial and municipal governments, as well as agencies, government business enterprises and the broader public sector.

Prior to joining Deloitte, Shelley had a 20-year track record of success as an entrepreneur running her own accounting practice. She was frequently engaged by the Office of the Auditor General of Ontario to assist with auditing the province's public accounts and performance audits.

Born in Saskatchewan, Shelley grew up in Alberta and graduated from the University of Alberta on the Dean's list with a Bachelor of Commerce degree. She obtained her Chartered Accountant designation at KPMG.

Day 1 Sessions

9:45 am – 10:45 am

A Reimagining Governance and Oversight Amid Digital Disruption

SESSION DESCRIPTION

In today's fast-paced business environment, it's essential for professionals to familiarize themselves with digital disruption and develop a deeper understanding of emerging technologies. This session is tailored to equip professionals with the knowledge necessary to effectively govern digital technologies within organizations while meeting the expectations of their Boards amidst the challenges and opportunities presented by emerging technologies.

The session will kick-off with an overview of the current digital landscape, highlighting six macro forces of information technology that are driving disruption. A key focus of the session will be on why these technology projects often fail when implemented and considerations to lower the risk of failure. A case study approach will offer practical insights and stimulate discussion on best leading practices for governing technology initiatives such as AI.

By the end of the session, participants will have an enhanced understanding of the governance challenges posed by digital disruption and will be better equipped to effectively manage and oversee their organization's digital initiatives, mitigate risks, and seize opportunities for growth and innovation in a way that aligns with organizational strategies and Board's expectations.

SPEAKER



Prashant Masand
Partner, Strategy, Risk & Transactions
Deloitte

Prashant is a Partner and co-leads AI governance nationally for Deloitte. He has been at the forefront of developing an AI related technology trust risk management and control framework, advising the federal government, and serving as a technical advisor on the development of AI standards in Canada and globally.

Prashant is also the national leader for Enterprise Risk Management and Board Governance Services. He serves as the outsourced Chief Audit Executive for a number of organizations and provides co-sourced internal audit services to various public and private clients. He is a trusted advisor to executives and Board members. He designs and delivers fit-for-purpose governance, risk and control solutions for organizations that want to play both defense and offense in a dynamic high-performance environment to empower them to achieve their strategic objectives and priorities.



Aby Mahmoud
Senior Manager, Audit & Assurance
Deloitte

Aby is a Senior Manager and lead's Deloitte's Digital Internal Audit practice nationally. Aby possesses more than a decade of proficiency in the domains of risk evaluation, data analytics and visualization, Continuous Controls Monitoring, Robotic Process Automation, Natural Language Processing, Machine Learning, Artificial Intelligence, management design, internal audit, and operational and risk management.

She has catered to a vast clientele in the private and public sectors, providing internal audit, advanced analytics, automation and AI, data visualization, governance and advisory services.

Day 1 Sessions

9:45 am – 10:45 am

So, you receive SOC Reports from your 3rd Parties; Now what?

SESSION DESCRIPTION

In today's interconnected business landscape, partnering with 3rd parties has become an operational necessity, and so has managing the associated risks. Stay ahead of potential pitfalls and learn about SOC Reporting services. SOC Reports promote transparency, providing you robust insights into your third-party vendors' control environments, safeguarding your business from unexpected security breaches and compliance issues.

Are you a SOC Report user recipient? Let's walk through a case study and refresh ourselves on how user management must review the report, including exceptions and assess the 'so what' for your particular environment, remind ourselves of the limitations of SOC reports (or the over dependence on SOC reports), recap the importance and responsibilities of users to perform CUECs (controls within the users realm to complement the SOC report controls), and the ongoing monitoring of user management with their 3rd parties to keep them accountable for exceptions and control gaps. Simply filing the SOC Report as part of your vendor management program is not an option!

SPEAKER



Sameera Jamal

Technology Risk,
Assurance Partner
EY

Sameera Jamal is an EY Technology Risk | Assurance Partner with 18+ years of experience in increasing stakeholder confidence via transparency into organization's financial and IT environments, through governance, risk and controls programs. She has a particular interest in third party controls evaluations for service organizations and has led third party risk assurance/attestation services covering CSAE3416 SOC1 (US SSAE18), CSAE3000 SOC2, CSAE3530 (Compliance Audits), and CSRS 4400 (Agreed Upon Procedures) with subject matter often covering both IT general controls and business process controls.



Matthew Batterton

Partner
EY

Matthew Batterton is an EY Partner with over 25 years of audit and consulting experience, focused on IT risk governance and internal control frameworks within the Technology Assurance practice. Matthew is EY's Canadian SOC Leader and has worked with CPA Canada in developing the Canadian SOC reporting standards to better meet the needs of service organizations and users. In addition, Matthew issues numerous SOC reports for some of the largest global organizations within Canada, as well as supporting organizations in interpreting the results of SOC reports and their impact.



Bronwyn Kemp

Senior Manager
EY

Bronwyn Kemp is a Senior Manager in the Technology Assurance practice of EY and has been with the firm for over 10 years. Bronwyn's time is spent leading external audit teams completing financial statement audits, Sarbanes Oxley compliance audits, and third-party service reporting – which includes helping her client's issue both SOC1 and SOC2 reports. She has a strong understanding of both issuing and reviewing SOC reports, and experience across industries, working with clients in Insurance, Financial Services, Government, and Technology. She is passionate about helping clients work through challenges, identify new and innovative solutions, and adjust to changing and evolving markets and regulatory landscapes.

Day 1 Sessions

11:00 am – 12:00 pm

A Navigating the Complexities of Data Risk in ESG

SESSION DESCRIPTION

Recent years have witnessed ESG regulators worldwide imposing ever evolving mandates on corporations. Canadian firms navigate a labyrinth of sustainability disclosure requirements based on guidelines by OSFI and the SEC, and broader requirements if they operate globally.

Efficient response to these emerging requirements requires transparency and trust over new sources of data, and establishing robust processes powered by leading technologies that support a forward-looking approach to ESG analytics and reporting.

This session delves into the escalating intricacies of data risk, with a keen focus on challenges associated with ESG data extraction, transformation, and reporting. Participants will explore strategies to harness synergies between people, processes, and technologies for effective ESG data management. We will also share insights on how Internal Audit and Risk/Compliance functions can bolster organizational readiness to accurately identify, assess, and disclose climate related risks and metrics.

SPEAKER



Mark Selvaratnam
Director, Digital Risk Solutions
PwC Canada

Mark is a director in PwC's Enterprise Systems and Emerging Technology Assurance practice. He is a technology and risk consulting professional with experience in helping clients establish trust in their systems and data through the design and implementation of automated compliance solutions. He has led and been involved with large technology transformations, including complex data transformation implementations, data governance reviews, data audits, and the development of large-scale data solutions aligned to external reporting requirements. Mark is a Chartered Professional Accountant (CPA) and holds a master's degree from the Rotman School of Management at the University of Toronto.



Belal Raifai
Manager, Digital Risk Solutions
PwC Canada

Belal is a Manager in the Digital Risk Solutions practice at PwC Canada Toronto office. He holds a master's degree in Accounting and a bachelor's degree in Life Sciences from the University of Toronto. Belal is a Chartered Professional Accountant (CPA) and a Certified Information Systems Auditor (CISA). He is also a certified Workday consultant, with a focus on Financial Management and Risk Advisory, assisting clients transform their finance function through the power of Cloud solutions. Belal has been leveraging his expertise in Data management to assist clients with their ESG journey, guiding them on how to best collect, analyze and report on vast amounts of ESG data, while adhering to standards and regulatory requirements.

B Product Security Testing to Combat Supply Chain Attacks

SESSION DESCRIPTION

What is Product Security Testing and how it can help combat against Supply Chain Attacks?

Overview on how organizations can build threat models around the hardware and software they use to build their solutions, and by leveraging Open Source Intelligence (OSINT), enumerate threats to building attack trees.

Demonstrate how this 'bottom up' threat analysis approach complements a top-down vulnerability assessment approach.

SPEAKER



Ismael Valenzuela
Vice President – Threat Research & Intelligence
BlackBerry

Ismael Valenzuela
CISM, CISSP, GSE, GCIH, GCIA, GPEN, GCUX, GCWN, GCFA, GMON, GREM, GSNA, GWAPT

Ismael is a Vice President – Threat Research & Intelligence at BlackBerry. He is a well-known and top-rated author & instructor for SANS, which reaches over 165,000 professionals globally. He has 60+ publications & talks that have been published in the last 4 years. He is also an IANS Research Faculty Member.

Day 1 Sessions

1:00 pm – 2:00 pm

A Re-inventing Second Line of Defense to Embrace Digital Disruption

SESSION DESCRIPTION

The pace of technological change worldwide is unprecedented. Now more than ever, sound risk management practices are essential to mitigate information security exposures arising from agile, dynamic, and rapid changes. Over the past decade, the Second Line of Defense (2LoD) function for Information Security has been vital in establishing robust risk management practices, enabling businesses to operate its digital assets within their risk appetite. However, it is crucial for 2LoD to evolve its practices to support the accelerated pace of technological change and disruption. This evolution is necessary to maintain business competitiveness while effectively managing risk. In this presentation, we will explore common pitfalls in risk management practices in the context of rapid technological change and discuss preferred alternatives for effectively managing risk while embracing digital disruption.

SPEAKER



Eduardo Delgado
Vice President- 2LoD Information Security Risk Management
TD

Cybersecurity risk executive with over twenty years of professional experience in information security, cybersecurity, risk management, and internal audit. I work as a Vice President in TD Bank as part of the Second Line of Defense function, leading the independent oversight and challenge of enterprise-wide Information Security risk management activities. Previously, I worked at Deloitte for more than ten years, leading many Cybersecurity management consulting projects, ethical hacking & red team operations, and IT control assurance engagements across multiple industries.

B Demand for Data Governance Programs in the Age of AI

SESSION DESCRIPTION

During this session you will learn and understand the key risks and concepts for Data Governance and AI including the following learning objectives and discussions:

- Key definitions of AI and Data Governance including application opportunities.
- What are the key risks associated with Data Governance and AI and how to mitigate those risks?
- Recognize Emerging Standards for AI Governance.
- Understand the AI implementation lifecycle and key factors.
- How Data Governance applies in an AI context and key areas for consideration.

SPEAKER



Michael Kostanecki
Associate Director, Team Lead,
Technology Risk & Audit,
Protiviti

Michael is a proven leader with over 17 years of Internal Audit and IT Consulting experience specializing in the areas of Cybersecurity Emerging Technologies (AI), Data Governance, and Third-Party Risk Management Assessments / Internal Audits. As an Associate Director in the Protiviti Toronto office, Michael plays a hands-on leadership role in the Technology Audit practice. He has a unique blend and a deep understanding of key technical IT and Cybersecurity risk areas coupled with a foundational business and accounting background delivering meaningful value add recommendations to clients.



Tarun Dhawan
Associate Director, Technology Risk & Audit
Protiviti

Tarun is an Associate Director in Protiviti's Internal Audit practice, where he specializes in Technology risk. With over a decade of experience in IT risk consulting, his expertise includes conducting internal and external audits, cybersecurity assessments, cloud security assessments, and third-party risk management. Tarun supports Protiviti's Next Gen Internal Audit initiatives particularly those centered around managing risks and controls associated with Gen AI. With a demonstrated history of success, he has collaborated with clients spanning diverse sectors such as financial services, mining, and manufacturing.

Day 1 Sessions

2:15 pm – 3:15 pm

A **Managing Risks in Digital Payments**

SESSION DESCRIPTION

The presenters of this session will provide attendees with an outline of risks and controls with respect to digital payments. The scope of the presentation will include the following:

- Transactional flows for selected electronic payment types: (such as bill payments, credit/debit card payments, pre-authorized payments, domestic wires, and cross border transfers).
- Key technological, cybersecurity and regulatory requirements of relevance to payment ecosystem participants.
- Considerations in defining an organization's operational and technological risk tolerances

SPEAKER



Benjamin Bernal
Director, Enterprise Data Protection
Scotiabank

Benjamin is a former regulatory policy maker and supervisor serving as the Managing Director, Operational and Technology Risk for CNBV Mexico; has with over 25 years of experience in financial services. At Scotiabank, he has held several Director positions with global responsibility for Retail Payments Risk, IT Regulatory Compliance, Cyber Security and Information Technology Risk Management. He currently leads the global governance, strategy, oversight, and advisory for the Enterprise Data Protection group.



Stephanie Slavik
Director, Governance & Oversight,
Enterprise Data Protection
Scotiabank

Stephanie has achieved over 14 years of progressive experience in capital markets, business banking, and cash management functions. Previously at HSBC Bank Canada, she was the Chief Control Officer & Head of Business Management for Global Payment Solutions. Since 2022, she has served as a Director with global responsibility for Enterprise Data Protection.

Day 1 Sessions

2:15 pm – 3:15 pm

▣ The Impacts of Artificial Intelligence on DevOps Security

SESSION DESCRIPTION

Organizations are increasingly embracing DevOps (a combination of practices, tools, and a cultural philosophy that aims to improve collaboration and communication between software development and IT operations teams) to automate processes, shorten development lifecycles, and deliver higher quality software faster. This presentation will:

- Briefly outline the nature and scope of DevOps and the emerging role of Artificial Intelligence (AI) on the information technology (IT) landscape
- Highlight the challenges faced by internal auditors, as well operational and cybersecurity risk specialists who must provide assurance on the effectiveness of controls relating to DevOps security for organizations heavily reliant on IT.
- Discuss how AI can automate tasks, improve efficiency, and enhance controls with respect to logical access control & segregation of duties, code quality & security, configuration management tools, infrastructure management with code repositories, version control & change management, pipeline execution monitoring, resource utilization & application health monitoring, scalable & resilient pipeline/infrastructure design, and integration of usability testing, code review, and analysis practices, and
- Briefly review potential risks associated with AI in DevOps security (such as: bias in algorithms, or security vulnerabilities in popular AI tools).

SPEAKER



Miguel Mendez
Generative AI Tech Lead
Deloitte

Miguel is a Generative AI technical leader in Deloitte's Omnia AI practice. His work is influenced by his experience in the Contact Centre AI (CCAI) space creating voicebots and chatbots for enterprise clients. With a background in software application development, he brings a unique perspective to his Machine Learning focused work. Lately his work has been around evaluating and testing GenAI applications.



Wissam Bashour
Senior Manager - Cyber Risk
Deloitte

Wissam is a cybersecurity professional, specifically focusing on Cloud security, AI security and DevSecOps. With a strong background in technology and a deep understanding of security principles, Wissam has successfully led numerous projects in these domains across various sectors. As a senior manager in the Cyber in Technology & Transformation practice at Deloitte Canada, Wissam has played a pivotal role in shaping secure cloud infrastructure strategies and architecture planning. Wissam's expertise extends to AI security, where he has demonstrated proficiency in security architecture, planning, and the development of secure code.

In addition to his AI security expertise, Wissam is well-versed in DevSecOps practices. He understands the importance of integrating security into the development and deployment processes, ensuring that applications and systems are resilient to attacks. Wissam emphasizes the need for continuous security testing and monitoring throughout the DevOps lifecycle, enabling organizations to identify and address security issues proactively.

Day 1 Sessions

3:30 pm – 4:30 pm

A **It's not Intelligence it's Functionality!!!!!!**

SESSION DESCRIPTION

The press and pundits have been prolific on discussing the dangers of General Artificial Intelligence and the multiple ethical and functional effects of current emerging technologies. This presentation attempts to focus on AI as applied to accounting and auditing, and its realities. It shows studies using machine learning and natural language processing, including generative efforts, and robotic and extended process automation. It concludes that a very promising set of applications is emerging, but there is little danger to most of us in the profession, although the impacts are going to be substantive.

SPEAKER



Dr. Miklos A. Vasarhelyi

KPMG Distinguished Professor of AIS
Rutgers Business School

Miklos A. Vasarhelyi [Ph.D in MIS (UCLA) MBA (MIT) and BS in Economics and Electrical Engineering (the State University of Guanabara and Catholic University of Rio de Janeiro)]. Professor Vasarhelyi is currently the KPMG Distinguished Professor of Accounting Information Systems and Director of the Rutgers Accounting Research Center (RARC) & Continuous Auditing and Reporting Laboratory (CARLAB) at Rutgers University. He has published more than 300 journal articles, 25 books, and directed over 60 PhD theses. He is the editor of the Artificial Intelligence in Accounting and Auditing series and the co-editor of the the International Journal or Digital Accounting..

Professor Vasarhelyi is credited with the original continuous audit application and as the leading researcher in this field. The CAR Lab's projects include among others AICPA's Radar, Siemens, KPMG, P&G, AICPA, CA Technologies, and Itau-Unibanco. Prof. Vasarhelyi has been awarded the Outstanding Educator of the year by the AAA in 2014, AICPA distinguished scholar in 2018, notable contributions to the accounting literature in 2021, and the Wasserman award by ISACA in 2013. His current work includes continuous prediction and intervention expansions on the CA schema, blockchain, smart contracts, process mining, and several machine learning projects.

Day 1 Sessions

3:30 pm – 4:30 pm

Secure Cloud Application Development with Container Orchestration on Google Cloud Platform

SESSION DESCRIPTION

The rapid adoption of cloud-based application development, coupled with the rise of container orchestration tools like Kubernetes, has revolutionized how businesses build and deploy software. However, this agile approach introduces unique security and risk management challenges. This session will explore the critical considerations for secure cloud application development within the Google Cloud Platform (GCP) ecosystem. We'll dive into the governance, oversight, and risk management implications that Boards of Directors and executive teams need to understand. We'll also dissect the differentiated responsibilities of Google Cloud (as the service provider) and your organization (as the service consumer) in maintaining a robust security posture.

Key Takeaways:

- **Case Studies:** Examine real-world (hypothetical) scenarios illustrating the consequences of security oversights in container orchestration, highlighting the importance of proactive measures and continuous monitoring.
- **Governance and Oversight:** Understand the crucial role of governance in mitigating risks associated with cloud application development and container security.
- **Shared Responsibility Model:** Clarify the distinct responsibilities of Google Cloud and your organization in ensuring secure cloud application practices.
- **Secure Development Best Practices:** Learn practical techniques for secure coding, data storage, and container permissions within the Google Cloud environment.

This session is ideal for IT risk professionals, security officers, and decision-makers responsible for cloud security and governance. Learn how to harness the power of Google Cloud while safeguarding your applications and data through secure container orchestration.

SPEAKER



Sarah Shafey

Delivery Executive (Cloud Services)
Google Cloud Consulting

A seasoned navigator of complex IT and business transformations, **Sarah Shafey** guides organizations through the intricate landscapes of portfolio, program, and risk management governance. With a keen eye for bridging the strategic and operational divide, Sarah empowers teams to translate vision into tangible action and driving productive outcomes. Sarah is an advocate for Diversity and Inclusion and fosters a culture of belonging and unlocking the potential of every team member.



Maulik Thaker

Delivery Executive
Google Cloud Consulting

A seasoned delivery leader distinguished for his expertise in spearheading large-scale, intricate Digital Transformation initiatives. With a proven track record of driving tangible results and fostering inclusive success, he stands as a prominent supporter for collaboration and diversity. Maulik's approach to work is marked by insightful analysis and pragmatic wisdom, offering teams a roadmap for navigating the complexities of digital transformation and empowering them to drive positive change within their organizations.



Paul Williams

App Modernization Engineer
Google Cloud Consulting

Paul is a software engineer who realized that most technology issues are not really technology issues, but rather people, process, and culture issues. Paul works to challenge organizations to create processes and cultures that allow software engineers to achieve high velocity and promote innovation while still honoring governance and quality requirements.

DAY 2: Thursday June 27, 2024	
7:45 – 8:20 AM	Registration and Continental Breakfast
8:20 – 8:30 AM	Welcome Remarks Margaret Lee-You, Conference Chair & Carlos Chalico, Secretary Toronto Chapter
8:30 – 9:30 AM	Keynote: Let's Talk About the Letter C Sami Houry Head, The Canadian Centre for Cyber Security
9:30 – 9:45 AM	BREAK
	STREAM A STREAM B
9:45 – 10:45 AM	<div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> Data Ethics in the age of GenAI Jesslyn Dymond - Director of Data Ethics TELUS </div> <div style="width: 45%;"> AI Confidence Index Yvonne Zhu, Partner, Technology Assurance, AI Assurance Lead EY </div> </div>
10:45 – 11:00 AM	BREAK
11:00 – 12:00 PM	<div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> The role of AI in the Battle of Good vs Evil – Who wins? Shil Sircar, SVP, Product Engineering & Data Science BlackBerry </div> <div style="width: 45%;"> Key Challenges in Managing Cybersecurity with Operational Technologies John Heaton, Partner Cybersecurity KPMG </div> </div>
12:00 – 1:00 PM	LUNCH
1:00 – 2:00 PM	<div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> Maximizing Cyber Risk Transfer Ruby Rai, Cyber Practice Leader, Canada Marsh Specialty US & Canada </div> <div style="width: 45%;"> The Hidden Dangers of Email Spoofing: How to Protect Your Organization from Costly Threats Irfan Aziz Hayat, Founder SecureMeNow.ca / TechGuru Behram Farooqh, Principal Farooqh Consulting </div> </div>
2:00 – 2:15 PM	BREAK
2:15 – 3:15 PM	<div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> Asset Management Automation - from an External and Internal Perspective Christine Dewhurst, Partner CloakIT Adam Rafael, VP Customer Experience UltraRed </div> <div style="width: 45%;"> Deepfakes and Cybersecurity: The Double-Edged Sword of AI Behram Farooqh, Principal Farooqh Consulting Irfan Aziz Hayat, Founder SecureMeNow.ca / TechGuru </div> </div>
3:15 – 3:30 PM	BREAK
3:30 – 4:30 PM	Massive AI with a Small Energy Footprint Samuel Mugel, PhD, CTO Multiverse Computing
4:30 PM – 4:45	Closing Remarks

Day 2 Keynote Session

8:30 am – 9:30 am

Let's Talk About the Letter C

SESSION DESCRIPTION

In today's interconnected world, robust cyber security is crucial as cyber threats grow in complexity. Join Sami Khoury, Head of the Canadian Center for Cyber Security, to learn about the Canadian cyber threat landscape and the vital role of collaboration among government, private sector, and international allies in developing effective cyber security practices. By working together, we can enhance resilience, protect sensitive information, and secure our digital future. Everyone has a role to play in combating cyber threats.

KEYNOTE SPEAKER



Sami Khoury

Head

The Canadian Centre for Cyber Security

Sami Khoury serves as the Head of the Canadian Centre for Cyber Security (the Cyber Centre), acting as the primary source of expert advice, guidance, services, and support on cyber security for government entities, critical infrastructure owners and operators, the private sector, and the Canadian public. Sami embarked on his career at the Communications Security Establishment (CSE) in 1992, initially as a research engineer specializing in the impact of emerging multimedia communications technologies. Over the years, he has held various operational and leadership roles at CSE. More recently, he served as Assistant Deputy Minister for Enterprise Technologies and Solutions. In this capacity, he was CSE's Chief Information Officer (CIO).

Additionally, Sami led CSE's comprehensive Research program and the 24/7 Operations Centre. Educationally, Sami holds a Bachelor's degree in Computer Engineering and a Master of Applied Science from Concordia University in Montreal. In 2016, he completed a certificate program in Public Sector Leadership at the University of Ottawa.

Sami's contributions have been recognized through various accolades, including the Queen Elizabeth Diamond Jubilee Medal and the APEX Award of Excellence for Innovation.

Day 2 Sessions

9:45 am – 10:45 am

A Data Ethics in the Age of GenAI

SESSION DESCRIPTION

Learn about the role of data ethics, trust and governance to support the rapid adoption of generative AI tools. This session will walk through the tools and drivers for GenAI policies in a North American context, and explore key considerations for use cases. Data ethics can provide a path for inclusive and diverse perspectives to shape responsible use of AI.

SPEAKER



Jesslyn Dymond
Director of Data Ethics
TELUS

Jesslyn Dymond is the Director of Data Ethics at TELUS, leading their world-class approach to responsible, data-driven innovation including the award-winning Responsible AI portfolio and the ISO-certified Privacy by Design Data for Good program. A recognized leader in data enablement and an advocate for creative solutions, she leverages her privacy and data governance expertise to build customer trust with emerging technology. Jesslyn completed a Master of Information from the University of Toronto's iSchool, is a Certified Information Privacy Professional/Canada (CIPP/C) and Data Ethics Professional from the Open Data Institute.

B AI Confidence Index – a Quantitative Risk Measurement Approach

SESSION DESCRIPTION

On this topic, we will speak to EY's AI Confidence Index which is a metric that quantifies the understanding of risks in the AI solutions, focusing on the responsible AI principles and weighted by associated impact of the AI system. We will look at how the Confidence Index can be leveraged throughout the AI governance framework, AI system lifecycle, the benefit of a quantitative approach, a use case measurement and demo video to see it live in action. This session will provide a new approach for organizations to measure and report the risk metrics of the AI systems, models, and enhance the effectiveness of its AI governance and risk management framework.

SPEAKER



Yvonne Zhu
Technology Assurance, AI Assurance
Lead | Partner
EY

Yvonne Zhu is EY Canada's AI Assurance Leader focusing on Responsible AI Risks and Controls. She has over 18 years of experience in risk management and IT auditing and a focused specialization in AI governance, risk and controls management and AI assurance since 2018. She is deeply committed to assisting organizations implement AI in an ethical and responsible manner and she played a pivotal role in the development of the EY Responsible AI Framework, AI principles, along with comprehensive risk and impact assessments. She facilitated the seamless execution of compliance audits and attestation methodology and was instrumental in leading readiness assessments against the NIST AI Risk Management Framework (RMF), EU AI Act, and ISO 42001 AIMS standard.

Day 2 Sessions

11:00 am – 12:00 pm

A | The role of AI in the Battle of Good vs Evil – Who wins?

SESSION DESCRIPTION

Can the forces of good use AI to enhance their defenses before the bad guys level-up their attacks?

Learn about the new risks and defenses to prevent data poisoning, carefully curate your data, and protect your AI Tools against new attacks that can fool models and corrupt your dataset.

SPEAKER



Shil Sircar
SVP, Product Engineering & Data Science
BlackBerry

Shiladitya (Shil) Sircar is the Senior Vice President, Product Engineering & Data Science at BlackBerry, where he leads Cybersecurity R&D teams.

He is responsible for the development of BlackBerry Cylance Threat Intelligence Cloud, ZTNA, NDR, and XDR platforms.

He holds many patents and publications in the fields of machine learning, mobile messaging, cryptography, satellite imaging, and radar interferometry.

Shil has a bachelor's and master's degree in Electrical and Communications Engineering from Memorial University of Newfoundland.

B | Key Challenges in Managing Cybersecurity with Operational Technologies

SESSION DESCRIPTION

Having built out their cyber security programs, hired key staff and engaged third parties to monitor and support their cyber security, and managed and secured their IT networks and devices, organizations are increasingly challenged to manage and secure the breadth of Industrial Internet of Things (IIOT) and Operational Technologies(OT), including video surveillance, networked smart devices, HVAC, elevators and security systems that have been implemented.

As the reliance on IIOT and OT increases, organizations are finding it challenging to keep up with the rapidly changing needs of their business and the impact cybersecurity has on each process and control. Audit committees, overseeing many of the company's activities and performance, must be certain management is keeping up with this evolving landscape.

Our session will cover the IIOT and OT specific cyber threats, the governance required to manage these solutions, and the challenge of securing, patching and monitoring these networks and devices.

SPEAKER



John Heaton
Partner, Cyber Security
KPMG

John Heaton, CA/CPA, CISA, CISSP

John is an experienced IT Risk and Security transformation leader with over 35 years of experience. He brings over 25 years of pragmatic experience in helping clients transform their IT risk and security organizations, solutions and processes to meet the ever changing regulatory and customer requirements.

Day 2 Sessions

1:00 pm – 2:00 pm

A Maximizing Cyber Risk Transfer

SESSION DESCRIPTION

As companies integrate digital technologies into business operations, cybersecurity risk can also increase. This presentation focuses on key considerations in optimizing your cyber insurance coverage and premiums. A case study will be used to illustrate a holistic approach for the greatest possible protection against a cyber-attack or breach. Attendees will understand how to determine the right amount of cyber insurance coverage needed to effectively recover from cybersecurity-related operational loss events.

SPEAKER



Ruby Rai
Cyber Practice Leader, Canada
Marsh Specialty US & Canada

As Marsh Canada's Cyber practice leader, **Ruby** is charged with ensuring Marsh delivers to its clients, customized solutions powered by actionable insights and analytics. Ruby has over 18 years of insurance experience, which includes managing Cyber & Professional Liability portfolio for a global insurance company and leading cyber broking practice for a Tier 1 brokerage in Canada.

In her role, Ruby helps clients understand, measure, and manage privacy and information security risks and finding the right solutions for risk transfer. She actively participates in public forums to promote the need for identifying and managing cyber risks.

Ruby is a certified Information Privacy Professional and holds her CRM designation.

Day 2 Sessions

1:00 pm – 2:00 pm

The Hidden Dangers of Email Spoofing: How to Protect Your Organization from Costly Threats

SESSION DESCRIPTION

Email spoofing is a major threat, with 94% of malware delivered via email and businesses losing over \$12 billion to email fraud annually. This session will uncover how attackers exploit email systems through sophisticated methods, revealing the true extent of potential consequences along with essential techniques needed to identify, prevent, and mitigate the impact of email spoofing. Attendees will understand the fundamentals of email spoofing, explore advanced monitoring / detection methods, and discover best practices for implementing email authentication protocols such as BIMI, SPF, DKIM, and DMARC.

Additionally, the session will include real-world case studies of email spoofing incidents and discuss effective mitigation techniques to minimize damage and recover swiftly. Join us for an in-depth discussion led by industry experts; and equip your organization with the knowledge and tools necessary to protect against email spoofing threats and prevent financial losses.

SPEAKER



Irfan Aziz Hayat

Founder

SecureMeNow.ca / TechGuru



Behram Farough

Principal

Farough Consulting

Irfan A. Hayat is a recognized leader in CyberSecurity & Innovation with over two decades of experience in cybersecurity and innovation. Passionate about his work, he spearheads whitehat hacking, IT design, delivery, and audit services for clients across various sectors, including government, healthcare, professional services, manufacturing, and education. Additionally, he serves as a vCIO/vCTO for multiple organizations, guiding businesses with combined annual revenues exceeding \$125 million.

Irfan was solely responsible for Whitehat identification of a Cyber Threat for a Bank with revenue exceeding 1 billion USD. He founded SecureMeNow.ca with a mission to protect Canadian organizations from email-based threats, particularly phishing and spoofing attacks. Beyond email security, he is dedicated to developing forward-thinking solutions that address new cybersecurity risks due to the risk of AI and deep fake technologies, ensuring that organizations remain ahead of emerging threats

Behram is a Chartered Accountant by profession, with over 30 years of experience that spans from the shop floor to the Board room, Behram has conducted assignments that consider the interplay, optimization and oversight of strategy, people, systems, and processes.

Behram has acquired highly developed skills in Information Technology by serving clients at the forefront of constantly evolving, disruptive and emerging technologies and has witnessed resultant business impact on digital trust and business transformation. Behram has served a diverse portfolio of clients in the Americas, Australia and EMEA region, in both public and private sectors.

Day 2 Sessions

2:15 pm – 3:15 pm

A **Asset Management Automation - from an External and Internal Perspective**

SESSION DESCRIPTION

Join us for an exhilarating session designed specifically for ISACA professionals, where we will explore how asset automation is set to transform IT governance. Discover the key concepts, benefits, and real-world applications of automation, and learn how it can enhance efficiency, accuracy, and security within your organization. Through case studies and a live demonstration, you will gain practical insights into implementing asset automation and overcoming common challenges, ensuring a seamless transition to this cutting-edge approach.

Prepare to be inspired by the future trends in asset automation, including the role of AI and machine learning, and understand how these innovations will shape the next decade of IT asset management. This session will empower you with the knowledge and tools to optimize operations, proactively manage risks, and stay ahead of the curve. Don't miss this opportunity to engage with experts, participate in interactive demos, and leave with actionable insights that will redefine your approach to IT governance. The future is automated, and it starts now!

SPEAKER



Christine Dewhurst

Partner
CloakIT

Christine is at the forefront of ushering in a new era of risk management programs. She actively champions the integration of cutting-edge tools in Artificial Intelligence (AI), automation and statistical analysis, aligning organizations with the transformative power of these technologies. She epitomizes the future of cyber leadership, blending her extensive experience with a forward-thinking approach to empower organizations in the ever-evolving landscape of cybersecurity and risk management.

With an impressive track record spanning over 27 years, Christine's journey through senior roles at renowned organizations, including KPMG, Deloitte, BMO, and Manulife, has solidified her reputation as an accomplished and collaborative leader. Her extensive expertise extends across multiple facets of Business, Technology, and Cybersecurity Assurance, proficiently fortifying Vulnerability, Identity & Access Management, and Business Resiliency capabilities.



Adam Rafael

VP, Customer Experience
UltraRed

Adam who is the VP of Customer Success and Technical Services at UltraRed, comes from a rich and extensive background in the cyber industry.

For over the last 20 plus years Adam has served in top technical units in military intelligence in the IDF, specifically concentrating on offensive and defensive cyber arenas, along with running multiple projects for not only the military but for the government, major financial institutions, and manufacturing companies.

Previous to UltraRed, Adam built and managed diverse global teams at HP Enterprise and at Cymulate along with consulting other security vendors and startups in their journey to build their Customer Success and technical offerings.

Day 2 Sessions

2:15 pm – 3:15 pm

B

Deepfakes and Cybersecurity: The Double-Edged Sword of AI

SESSION DESCRIPTION

Deepfake technology, utilizing advanced AI to create realistic but fraudulent videos, audio, and images, poses a serious threat to cybersecurity. This session will delve into the technology behind deepfakes, the risks they present, and recent incidents that highlight their impact, such as a deepfake scam that resulted in a \$243,000 loss for a UK company and another that led to a \$25 million fraud. Participants will gain insights into how to detect and counter such threats using available technology coupled with must-have practical strategies.

SPEAKER



Behram Faroogh

Principal
Faroogh Consulting

Behram is a Chartered Accountant by profession, with over 30 years of experience that spans from the shop floor to the Board room, Behram has conducted assignments that consider the interplay, optimization and oversight of strategy, people, systems, and processes.

Behram has acquired highly developed skills in Information Technology by serving clients at the forefront of constantly evolving, disruptive and emerging technologies and has witnessed resultant business impact on digital trust and business transformation. Behram has served a diverse portfolio of clients in the Americas, Australia and EMEA region, in both public and private sectors.



Irfan Aziz Hayat

Founder
SecureMeNow.ca / TechGuru

Irfan A. Hayat is a recognized leader in CyberSecurity & Innovation with over two decades of experience in cybersecurity and innovation. Passionate about his work, he spearheads whitehat hacking, IT design, delivery, and audit services for clients across various sectors, including government, healthcare, professional services, manufacturing, and education. Additionally, he serves as a vCIO/vCTO for multiple organizations, guiding businesses with combined annual revenues exceeding \$125 million.

Irfan was solely responsible for Whitehat identification of a Cyber Threat for a Bank with revenue exceeding 1 billion USD. He founded SecureMeNow.ca with a mission to protect Canadian organizations from email-based threats, particularly phishing and spoofing attacks. Beyond email security, he is dedicated to developing forward-thinking solutions that address new cybersecurity risks due to the risk of AI and deep fake technologies, ensuring that organizations remain ahead of emerging threats

Day 2 Sessions

3:30 pm – 4:30 pm

A **Massive AI with a Small Energy Footprint**

SESSION DESCRIPTION

Deep learning is increasingly at the heart of everything we do. Applications powered by AI, including large language models like ChatGPT, can create high-quality custom content and even write functional code. However, the environmental costs of training deep learning with its energy-intensive requirements are rapidly growing.

My talk will present our work on tensor networks, which improve training efficiency without compromising accuracy. They advance the resolution of extremely complex problems by extending computational capabilities beyond the capability of even the most sophisticated algorithms running on the best supercomputers.

SPEAKER



Sam Mugel, PhD

CTO

Multiverse Computing

Sam Mugel is CTO and co-founder at Multiverse Computing. He is an Expert in quantum computing and quantum machine learning. His PhD is jointly awarded by ICFO (Spain) and the University of Southampton (UK). Formerly, he was Computational physicist at Cortirio (UK), Technical Director at The Quantum Revolution Fund, and Founder and CTO at Groundstate Consulting. He is an Advisor for the McKinsey Tech Council and the Forbes Tech Council, and Mentor at the Creative Destruction Lab.

**We would like to acknowledge our 2024 Summer Conference
Platinum Sponsor EY
for hosting this year's in-person conference**



Thank You!

We would like say thank you to our 2024 Summer Conference Planning Committee members & Volunteers

2024 Conference Planning Committee

Margaret Lee-You - Chair
Asif Mohammed
Behram Faroogh
Belal Raifai
Carlos Chalico
Najib Hayat
Nick Pawliwec
Rakhi Henderson
Rashna Daroga
Rob Mitchell
Russell Dyer

2024 Conference Planning Committee Volunteers

Daraius Variava
Harsh Sahni
Nihar Mishra
Noor Tabbassum
Rick Murphy

Thank You!