Deloitte.

Intermountain Health

MARSH

2026 Cybersecurity Healthcare Education Summit

July 15 to 17, 2026

Blair Education Center at Intermountain Park City Hospital

Program agenda

Wednesday, July 15, 2026 – Day 1

Start Time	End Time	Presentation Name	Speaker
7:00 AM	8:00 AM	Registration & Check In	
8:00 AM	8:30 AM	Breakfast & Networking	
8:30AM	9:15 AM	Opening Remarks	Erik Decker
9:15 AM	10:00 AM	Cybersecurity Signals – Connecting Controls and Incident Outcomes	Matt Berninger
10:00 AM	10:30 AM	Morning Break	
10:30 AM	11:30 AM	AI in Security: Expert Panel Discussion	Andrew Douglas, Jim Aldridge, Derek McGhie, David Burrell
11:30 AM	12:00 PM	Transition / Networking	
12:00 PM	1:00 PM	Lunch / Lightning Talk	Proofpoint and Beazley Security
1:00 PM	1:45 PM	The Awareness Illusion: Why our Human Controls keep failing	Alexandra Panaretos
2:00 PM	3:00 PM	Breakout Session - Cyber Resilience in Healthcare: A CISO Dialogue	Dan Bowden, Jim Aldridge, Erik Decker
2:00 PM	3:00 PM	Breakout Session - Key trends and mitigations related to AI-enabled attacks and defense	Nathan Moon
3:00 PM	3:30 PM	Afternoon Break	
3:30 PM	4:30 PM	Panel: Inside the Mind of an Underwriter	Meredith Schnur, Andrew Cross, Elizabeth Springer, Peter Baxter
4:30 PM	5:00 PM	Daily Recap	Meridith McGlincy
5:00 PM	6:30 PM	Happy Hour	

Program agenda

Thursday, July 16, 2026 – Day 2

Start Time	End Time	Presentation Name	Speaker
7:30 AM	8:30 AM	Breakfast & Networking	
8:30 AM	9:00 AM	Opening Remarks & Day 1 Recap	Raj Mehta
9:00 AM	10:00 AM	How AI is changing threat Landscape	Chuck Littmann and Andrew Douglas
10:00 AM	10:30 AM	Morning Break	
10:30 AM	11:30 AM	AI for Cyber and Cyber for AI	Naresh Persaud
11:30 AM	12:00 PM	Transition / Networking	
12:00 PM	1:00 PM	Lunch / Lightning Talk	CodeIntegrity.ai and Resilience
1:00 PM	2:00 PM	Experience as a clinician on utilizing AI	Dr. Tamara Moores Todd
2:00 PM	3:00 PM	FBI Cyber Threat Brief: Protecting Healthcare Systems from Emerging Threats	Michael G. Cahoon
3:00 PM	3:30 PM	Afternoon Break	
3:30 PM	4:30 PM	Women in Cyber Panel Discussion on AI	Meredith Schnur, Lisa Bisterfeldt, Katie Conner, Alexandra Panaretos
4:30 PM	5:00 PM	Daily Recap & Announcements	Paige Ishii
5:00 PM	6:30 PM	Happy Hour	

Program agenda

Friday, July 17, 2026 – Day 3

Start Time	End Time	Presentation Name	Speaker
6:30 AM		Intermountain Hosted Hike	
7:00 AM	8:00 AM	Breakfast & Networking	
8:00 AM	8:45 AM	Know your Adversary: Identity Threats, Social Engineering, and Frontier AI Threats in Healthcare	Todd Felker and Steve Dahl
9:00 AM	10:00 AM	TTX A Disturbance in the Network: A Ransomware Micro TTX	Brian McCormack
10:00 AM	10:30 AM	Morning Break	
10:30 AM	11:30 AM	The Rise of Resilience: Minimum Viable Hospital, Isolated Recovery Environment & Systemic Risk	Rob Panunzio, Jim Lamadrid, Max Parkinson, Richard Price
11:30 AM	12:00 PM	Closing Remarks	Dan Bowden

Day 1 Speakers

Speakers

Erik Decker
Intermountain Health
VP and Chief Information Security Officer

Bio: Erik Decker is Vice President and Chief Information Security Officer at Intermountain Health, where he leads information security for the multi-state health system. He brings 26 years of IT experience, including 19 years in information security.

He has led major healthcare cybersecurity efforts, including the Healthcare Sector Coordinating Council's Joint Cybersecurity Working Group and HHS's 405(d) task group, and co-authored key industry publications such as Health Industry Cybersecurity Practices and the Hospital Resiliency Landscape Analysis.

Erik has received multiple honors for cybersecurity leadership, has testified before Congress, and advises on national healthcare cybersecurity policy. He holds a master's degree in information technology from Loyola University Chicago, a bachelor's degree in cell and structural biology from the University of Illinois, and a Digital Directors Network QTE certification.

Matt Berninger
Marsh
Senior Vice President

Bio: Matt Berninger is the head of Cyber Data Services at Marsh. In this role he performs cybersecurity research, builds predictive cyber models, and advises customers on cybersecurity decisions. During his 15+ years in cybersecurity he has led teams in Incident Response, Detection and Response, and Data Science within Private Industry, US Government, and the US Military. He lives in Denver CO and enjoys the outdoors, dogs, and math.

Speakers

Andrew Douglas
Cyber Risk Services
Deloitte
Managing Director

Bio: Andrew has over 25 years with Deloitte member firms globally, including in New Zealand, the United States, and the Cayman Islands. I am a Managing Director in the Cyber group, working in the Infrastructure security team, and focused on attack surface management and offensive security I currently lead our firm's Hybrid-Operate Attack Surface Management team (which is amazing - ask me about it!) as well as serving clients across Cyber Infrastructure security.

Jim Aldridge
Marsh
SVP, Cybersecurity Advisor

Bio: Jim Aldridge brings an operator's depth and an executive's perspective to cyber risk management. Over two decades, he has led incident response for global enterprises under attack by state-sponsored and financially motivated adversaries, briefed boards mid-crisis, and seen the network through an attacker's eyes as a penetration tester.

Today he is a Cybersecurity Advisor at Marsh, where he helps CISOs navigate cyber risk, leveraging its proprietary analytics that combine insights from actual losses to inform control prioritization. A licensed private pilot, Jim applies an aviator's discipline – situational awareness and respect for failure modes – to how organizations manage risk.

Speakers

David Burrell
Intermountain Health
Cybersecurity Consultant

Bio: David Burrell is a Cybersecurity Consultant on the Cybersecurity Architecture team at Intermountain Health with 27 years of experience spanning system administration, enterprise infrastructure, and information security. He specializes in the security architecture of cloud workloads, artificial intelligence systems, and Payment Card Industry (PCI) environments, and leads key initiatives to strengthen the security of critical systems across Intermountain, helping protect patient data while enabling the responsible advancement of technology. Beyond his professional work, David volunteers at local security conferences, contributing to greater awareness of cybersecurity and privacy in healthcare systems.

Derek McGhie
Intermountain Health
Application Security Consultant

Bio: Derek McGhie is an Application Security Consultant at Intermountain with a background spanning application security leadership, secure software development, and military intelligence. His experience includes building and improving secure software development lifecycles, guiding engineering teams through risk-based security practices, reviewing application architectures and code for vulnerabilities, and helping organizations balance security, delivery, and practical engineering constraints. His military intelligence background adds a strong foundation in analysis, risk assessment, data handling, and mission-focused decision-making, which informs his perspective on emerging AI security challenges such as trust, accountability, misuse, and secure adoption.

Speakers

Alexandra Panaretos
Tenet Healthcare
Director of Governance, Regulatory Compliance and Security Awareness

Synopsis: Despite growing investment in cybersecurity awareness and training, many programs still create risk instead of reducing it. In this session, we'll examine why one-size-fits-all approaches fail and how to design human risk programs that are role-based, risk-aligned, and behavior-driven. We'll also look at how AI, communication strategy, and real-world usability affect program effectiveness. Whether you're building a new program or improving an existing one, this session offers practical guidance to move from awareness to real risk reduction.

Bio: Alexandra Panaretos is a cybersecurity leader with nearly 20 years of experience in human-behavior cyber risk. She builds programs that strengthen security culture, reduce insider threats, and improve behavior-based risk mitigation and digital literacy.

Alex has spoken at SecureWorld, RSA Conference, NCA, and SANS on topics including social engineering and behavior-based security. She previously led Secure Culture Activation for EY Americas and served as Director of Professional Services at Proofpoint, bringing a background that blends cybersecurity, media, and behavioral insight.

She has built executive security, insider-threat, and incident response programs for Fortune 50 and Fortune 100 companies and holds an OPSEC Manager II certification. She also volunteers to educate communities on online safety and social media risks.

Dan Bowden
Marsh
Principal

Bio: Dan Bowden is a Chief Information Security Officer and cybersecurity executive with more than 30 years of experience leading security programs across healthcare, financial services, insurance, higher education, retail, and the military. He currently serves as Global Business CISO at Marsh, helping guide enterprise security strategy in a complex global environment.

Dan specializes in translating cyber risk into practical executive action, with deep focus areas including AI security, phishing-resistant identity, cyber resilience, supply-chain risk, third-party risk, and incident readiness. He is passionate about helping organizations move beyond compliance-driven security toward programs that measurably reduce real-world risk.

Dan brings a practitioner's perspective on today's healthcare cybersecurity challenges, including social engineering, business email compromise, AI-enabled threats, human behavior, and the controls that most influence incident outcomes.

Speakers

Nathan Moon
Intermountain Health
Sr Director of Fusion Center

Bio: Nathan Moon is the Senior Director of Intermountain Health's Cyber Fusion Center. Nathan is a well-respected speaker and security expert who has presented at several industry security conferences. At Intermountain, Nathan is responsible for all aspects of the organization's security detection and response activities. Nathan's experience covers a wide range of security specialties—incident management, identity management, security architecture, and security policy and procedure. He's excelled at Intermountain, designing an identity management framework, defining an overall security architecture process, and implementing their 24/7 Cyber Fusion Center with incident response, vulnerability and threat hunting. For more than 29 years, Nathan has been involved in information technology and security. Prior to his current role, Nathan worked in other areas of the Cybersecurity Department.

Meredith Schnur
Marsh
Managing Director

Bio: Meredith Schnur is the US and Canada Regional Cyber Practice Leader for Marsh. In this role, Meredith leads all operations in the US and Canada and is responsible for driving superior client service and operational excellence at every level of Marsh's Cyber Practice. She also works with Marsh's national and zonal distribution leaders to streamline and enhance Marsh's cyber operating model. Prior to joining Marsh, Meredith was the National Practice Leader of the Professional Risk Practice at Wells Fargo Insurance. Throughout her 30-year insurance career, she has focused solely on Errors & Omissions coverage and its subsequent evolution into Cyber insurance, and is a nationally recognized expert on Cyber, Media and E&O insurance.

Speakers

Andrew Cross
Resilience
SVP, Northwest Underwriting Manager

Bio: Andrew Cross is SVP and Regional Underwriting Manager at Resilience, a high-growth cyber risk management firm redefining how organizations approach cyber insurance. Resilience pairs top-rated insurance coverage with proprietary security software that translates an organization's security posture into quantified financial risk, giving CISOs and risk managers a shared language to prioritize investments and demonstrate impact to the board. Andrew brings over 12 years of cyber underwriting experience, including extensive work with healthcare organizations navigating an increasingly hostile threat landscape. He leads a regional team of cyber underwriters and partners with brokers to bring Resilience's Edge platform to organizations looking to connect their security programs to quantified financial outcomes. He previously spent seven years underwriting Technology E&O and Cyber Risk at CNA Insurance and is based in San Francisco.

Elizabeth Springer
Beazley Security
Northeast Regional Manager & US Private Equity Lead

Bio: Elizabeth Springer serves as Northeast Regional Manager for Cyber Risk at Beazley USA, leading the firm's largest U.S. region, spanning from Maine to Virginia. In this role, she is responsible for driving regional strategy, performance, and growth across the cyber portfolio, partnering closely with brokers and clients to deliver tailored solutions across a diverse and complex market. She has a specialized focus on large healthcare organizations, a segment that represents a significant portion of the Northeast book, bringing deep expertise to the unique cyber and technology risks facing the sector.

Elizabeth also serves as the U.S. Private Equity Lead for Cyber Risk, where she is responsible for driving the firm's national cyber strategy for sponsor-backed organizations. She develops and scales differentiated cyber solutions for private equity portfolios, aligning underwriting frameworks, distribution strategy, and product innovation to meet the evolving risk profiles of PE-backed companies. Through this work, she has delivered meaningful portfolio growth through tailored solutions and disciplined execution.

Speakers

Peter Baxter
Intermountain Health
Chief Risk Officer

Bio: Peter J. Baxter serves as Chief Risk Officer for Intermountain Health. He brings more than 20 years of experience as a corporate healthcare attorney, with deep expertise in medical malpractice, compliance, and risk management.

Peter earned a bachelor's degree in accounting from Brigham Young University and a Juris Doctor from Wake Forest University School of Law.

Before joining Intermountain, Peter practiced medical malpractice and healthcare law at Strong & Hanni in Salt Lake City.

Meridith McGlincy
Intermountain Health
Cybersecurity Training & Education Consultant

Bio: Meridith McGlincy, a behavior warrior, works as a passionate cybersecurity professional dedicated to safeguarding healthcare systems. She empowers caregivers to defend against ransomware, foster awareness, improve reporting, and promote vigilance to protect patient data and provide uninterrupted care. Honored with the Patriot award, she aligns cybersecurity strategies with organizational goals.

Day 2 Speakers

Speakers

Raj Mehta
Cyber Risk Services
Deloitte
Partner

Bio: Raj is a Partner with Deloitte Advisory's Cyber Risk Services. Raj currently leads the Cyber Security Operate and GRC Practice within the Life Science and Health Care industry sector across the US. Raj has ~thirty (30) years of experience in the field of information governance, security, privacy, risk management and compliance within the Healthcare space.

His experience includes performing risk assessments, as well as assessing, developing, and implementing strategies and solutions associated with information security and privacy matters.

Naresh Persaud
Cyber Risk Services
Deloitte
Principal

Bio: Naresh Persaud is a Principal in Deloitte Cyber, focused on cybersecurity across industries. He serves as Deloitte's Frontier AI Cyber practice leader, helping clients secure AI adoption and transform the cyber function. He has over 25 years of cybersecurity experience, including Identity and Management and Data Security. He has spent much of his career in the security software market, shaping industry-leading offerings and implementing security solutions in highly complex client environments. Previously, he served as the US Digital Identity Leader, helping clients transform identity and access programs to achieve better security controls.

Speakers

Chuck Littman
Cyber Risk Services
Deloitte
Managing Director

Bio: Chuck has leveraged 26 years of naval operational, intelligence and defensive cybersecurity experience protecting national interests and 10+ years of cybersecurity consulting experience. Chuck has built and leads Deloitte's Attack Surface Management (ASM) defensive cross-industry teams, designing, building, maturing and operationalizing programs at scale. He has facilitated secure organizational operations and mission success by continuously mapping, managing, and minimizing organizational threat exposure by focusing on true risk.

Andrew Douglas
Cyber Risk Services
Deloitte
Managing Director

Bio: Andrew has over 25 years with Deloitte member firms globally, including in New Zealand, the United States, and the Cayman Islands. I am a Managing Director in the Cyber group, working in the Infrastructure security team, and focused on attack surface management and offensive security I currently lead our firm's Hybrid-Operate Attack Surface Management team (which is amazing - ask me about it!) as well as serving clients across Cyber Infrastructure security.

Speakers

Dr. Tamara Moores Todd

Intermountain Health

Chief Health Informatic Office and Emergency Physician

Bio: Dr. Tamara Moores Todd is Chief Health Informatics Officer and an emergency physician at Intermountain Health, where she leads digital health strategy, clinical informatics, and technology-enabled workflow redesign to improve the patient and caregiver experience. With more than a decade of experience in clinical leadership, health IT, and medical education, she has built and led high-performing teams focused on scalable, human-centered innovation and better patient outcomes.

She earned her MD from Loma Linda University School of Medicine, completed emergency medicine residency at the University of Utah, and completed a fellowship in Clinical Informatics. Triple board certified in Emergency Medicine, Clinical Informatics, and Healthcare Administration, Leadership, and Management, she is also recognized for her work in clinical process improvement and digital health leadership. Her honors include #1 on Top Women in Leaders in Healthcare 2025 and Utah HIMSS Mental Health Leader of the Year 2023.

Michael G. Cahoon

Federal Bureau of Investigation

Cyber Special Agent

Bio: Michael G. Cahoon joined the FBI in 2008 and is currently assigned as a Cyber Special Agent in the Salt Lake City Division, Boise Resident Agency. Special Agent Cahoon covers the Cyber portfolio for the State of Idaho. He works closely with business, government, law enforcement, and intelligence partners to further the FBI Cyber mission. He investigates criminal activity on the darknet, criminal computer intrusions, and national security computer intrusions. Previously he worked in the Sacramento Field Office on Cyber and High-Tech Organized Crime squads, Cyber Division headquarters Liaison Officer, International Operations Division Program Manager, and Cyber Assistant Legal Attaché in LEGAT Madrid.

Speakers

Meredith Schnur
Marsh
Managing Director

Bio: Meredith Schnur is the US and Canada Regional Cyber Practice Leader for Marsh. In this role, Meredith leads all operations in the US and Canada and is responsible for driving superior client service and operational excellence at every level of Marsh's Cyber Practice. She also works with Marsh's national and zonal distribution leaders to streamline and enhance Marsh's cyber operating model. Prior to joining Marsh, Meredith was the National Practice Leader of the Professional Risk Practice at Wells Fargo Insurance. Throughout her 30-year insurance career, she has focused solely on Errors & Omissions coverage and its subsequent evolution into Cyber insurance, and is a nationally recognized expert on Cyber, Media and E&O insurance.

Lisa Bisterfeldt
St. Luke's Health
Cyber Resiliency Manager

Bio: Lisa Bisterfeldt leads the Cyber Resilience program at St. Luke's Health System in Boise, Idaho, where she strengthens the organization's ability to withstand and recover from cyber threats in support of its mission to improve community health. Her work focuses on incident response, business continuity planning, and backup and disaster recovery strategies that improve organizational preparedness and resilience.

Lisa brings a distinctive background to cybersecurity, with eight years of prior experience in emergency management across healthcare and government. She previously served as Emergency Manager for St. Luke's Health System, where she developed system-wide disaster response plans, incident command structures, and a HAZMAT program recognized as an industry best practice. She holds a Bachelor of Health Science Studies from Boise State University, a Master of Public Health from Idaho State University, and is a Certified Cyber Resiliency Professional (CCRP). Lisa is also an active member of the Health Sector Coordinating Council's Cyber Working Group, helping advance cyber maturity and preparedness across the healthcare sector.

Speakers

Katie Conner
Intermountain Health
Senior Director, Cybersecurity Assurance

Bio: Katie Conner is Senior Director of Cybersecurity Assurance at Intermountain Health, with more than 20 years of experience leading cybersecurity operations and GRC programs in complex healthcare environments. She is known for building strong enterprise security programs and advancing cyber resilience while enabling patient care and innovation. Katie holds a master's degree in Information Technology from the University of Denver. She previously served as an Adjunct Professor at the University of Denver, where she created and taught Information Security for Healthcare in the graduate program.

Alexandra Panaretos
Tenet Healthcare
Director of Governance, Regulatory Compliance and Security Awareness

Bio: Alexandra Panaretos is a cybersecurity leader with nearly 20 years of experience in human-behavior cyber risk. She builds programs that strengthen security culture, reduce insider threats, and improve behavior-based risk mitigation and digital literacy.

Alex has spoken at SecureWorld, RSA Conference, NCA, and SANS on topics including social engineering and behavior-based security. She previously led Secure Culture Activation for EY Americas and served as Director of Professional Services at Proofpoint, bringing a background that blends cybersecurity, media, and behavioral insight.

She has built executive security, insider-threat, and incident response programs for Fortune 50 and Fortune 100 companies and holds an OPSEC Manager II certification. She also volunteers to educate communities on online safety and social media risks.

Speakers

Paige Ishii
Intermountain Health
Cybersecurity Training & Education Senior

Bio: Since 2017, Paige has been instrumental in changing cultures from one of compliance to one that embraces cybersecurity with results-driven data. Her drive to continuously improve training & education program is centered on delivering top notch industry results while staying in alignment with organizational mission, vision, and values.

Day 3 Speakers

Speakers

Todd Felker
CrowdStrike
Healthcare Strategist

Bio: Todd has 30 years of Healthcare leadership and as CISO at Torrance Memorial he spent a decade building a Security Program from scratch. He has a proven track record of reducing organizational risk, and breaking down departmental silos. As a Security Leader with a knack for identifying disruptive technologies, he was CrowdStrike's first Healthcare Customer. He is now serving as an Executive Strategist for CrowdStrike, and enjoys helping other leaders with improving their cybersecurity posture and reducing cyber risk. In 2025, Todd became an advisor to the Health Sector Coordinating Council Cybersecurity working group, and is also an adjunct instructor for UT Austin.

Steve Dahl
Intermountain Health
Cybersecurity Manager

Bio: Steve Dahl is a cybersecurity leader at Intermountain Health with over 20 years of experience securing complex healthcare environments. He specializes in data protection, identity, and endpoint security, leading initiatives that strengthen HIPAA compliance and reduce risk across large healthcare systems. Known for translating complex security challenges into practical, patient-centered solutions, Steve brings a collaborative approach and a strong focus on enabling secure, high-quality care delivery.

Speakers

Brian McCormack
Intermountain Health
Governance & Business Resilience Manager

Bio: Brian McCormack is a cybersecurity and resilience leader with deep experience across healthcare technology operations, business continuity, disaster recovery, and cyber preparedness. He focuses on healthcare resilience strategy, operational continuity, and integrating cybersecurity capabilities across clinical and enterprise environments.

Brian leads initiatives in resilience engineering, healthcare continuity planning, tabletop and functional exercises, and recovery strategy development. His work includes Minimum Viable Hospital (MVH) planning and operational recovery frameworks, with an emphasis on aligning cybersecurity, infrastructure, clinical operations, and executive leadership response during disruptive events.

He holds a DBA, MSIM, and CISSP; he has presented at industry forums including CHIME, ServiceNow Knowledge, national industry conferences, and the Healthcare Education Summit.

Rob Panunzio
Intermountain Health
Cybersecurity Principal

Bio: Rob Panunzio is a Cybersecurity Principal on the Cybersecurity Governance and Business Resilience team at Intermountain Health, with over 19 years of experience in healthcare IT, cybersecurity, and resilience. He specializes in disaster recovery (DR), business continuity management (BCM), and resilience planning in complex healthcare environments.

Rob leads enterprise DR testing initiatives, supports tabletop exercises, and develops operational playbooks aligned to NIST and HICP frameworks. He is actively involved in advancing the Minimal Viable Hospital (MVH) framework, helping ensure continuity of critical clinical operations during cyber and operational disruptions.

Speakers

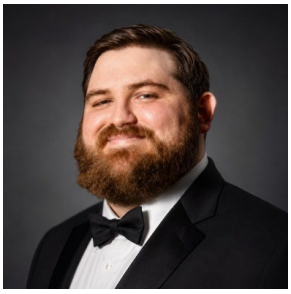
Jim Lamadrid
Intermountain Health
Cybersecurity Consultant

Bio: Jim Lamadrid is a Cybersecurity Consultant and Systemic Risk Team Lead at Intermountain Health with over 20 years of experience across government and private sectors. A former Supervisory Special Agent who led the FBI's Salt Lake City Cyber Task Force, he now specializes in healthcare resilience, systemic risk, and operational continuity. Jim holds an MBA in Data Analytics from Colorado Technical University, previously served in the U.S. Air Force Security Forces, and currently serves as an Information Warfare Officer in the U.S. Navy Reserves supporting national defense operations.

Max Parkinson
Intermountain Health
Cybersecurity Senior

Bio: Max Parkinson is a Cybersecurity Senior specializing in systemic risk at Intermountain Health, where he has spent the past four years monitoring and mitigating threats in the Fusion Center operations in complex healthcare environments, currently focusing on enterprise systemic risk after earlier experience in vulnerability management and penetration testing. Max holds a bachelor's degree in Cybersecurity, maintains a CISSP, and is certified in web application penetration testing.

Speakers



Richard Price
Intermountain Health
Cybersecurity Consultant

Bio: Richard Price is a Principal Cybersecurity Analyst at Intermountain Health, where he focuses on business continuity, disaster recovery, and helping the organization stay resilient when the unexpected happens. With more than 15 years of experience across cybersecurity, IT, and project management, he's known for translating complex risk and recovery concepts into practical plans people can actually use. Richard holds a Master of Science in Cybersecurity and Information Assurance and an MBA, along with certifications including CISSP, CISM, and PMP. He's also passionate about professional development and mentoring, helping others build the skills and confidence to grow in their own careers.

Deloitte.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms or their related entities (collectively, the "Deloitte Network"), is, by means of this communication, rendering professional advice or services. Before making any decisions or taking any action that may affect your finances, or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.

Copyright © 2026 Deloitte Development LLC. All rights reserved.