Monday, November 17, 2025

Top 10 risk and compliance related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next.

An AI agent is a system that can autonomously perceive, decide, act, and adapt … but seriously, why do we call them *agents*?

They do not wear suits and they do not earn commissions. They do not even qualify as secret agents, even when half the time, nobody really knows what they're doing behind the scenes.

The word *agent* comes from two traditions, computer science and law.

In computer science, the term *agent* was adopted in the late 1980s to describe autonomous software that could sense the environment and act. This marked a shift from traditional software, which generally followed explicit, step-by-step instructions, to programs that could operate more independently. Researchers in artificial intelligence, distributed systems, and robotics began to explore the idea that software could be designed not just to execute commands, but to pursue goals.

The term agent was inspired from the human concept of agency (acting on someone else's behalf). The important distinction was autonomy. An agent did not require constant supervision, and it could adapt its behavior to changing circumstances.

In law, an agent is a person who has been given the authority to act on behalf of another (the principal), in dealings with third parties. The essence of agency is representation. The acts of the agent, when performed within the scope of their authority, are legally binding on the principal, as if the principal had performed them directly.

The term *agent* is used for AI because it steps into a role that looks a lot like a human assistant. It does things on our behalf, without asking permission every five seconds.

There is no single, universally binding legal definition, for the term AI agent. In risk and compliance, the term is used by analogy to the law of agency. AI agents execute tasks on behalf of an identified principal, with real consequences for rights, obligations, and risk.

The choice of the word agent is deliberate. The law looks past the machine to the humans and entities who specify objectives, set constraints, provide access, and benefit from outcomes.

It is useful to distinguish AI agents from traditional automation.

Conventional scripts, robotic process automation, and fixed-rule workflows execute predefined steps under direct human orchestration.

AI Agents differ in three respects.

1. Dynamic perception. Agents maintain an ongoing, adaptive awareness of their environment. They continuously interpret signals from users, external data sources, sensors, APIs, or other systems.

This allows them to update their internal model of the world as conditions change, much like a human analyst who keeps revising an assessment when new information arrives.

2. Context-sensitive decision-making. Agents evaluate the current state, their objectives, and possible actions, then select among alternative courses to progress toward a defined goal. This resembles how a strategist weighs multiple pathways rather than blindly executing a prewritten script.

3. Operational autonomy. Agents can plan and execute multi-step workflows without human micromanagement. They act like a field operative who can figure out the next step on their own, escalate when needed, and keep pushing toward the objective. This increases the value, of course, but it also expands the surface area for legal and operational risk.

Each capability introduces a control challenge, like least-privilege access, credential management, confidentiality, data minimization. Multi-agent collaboration complicates attribution, logging, and explainability.

Because the legal system ultimately assigns responsibility to people and entities, the critical governance problem is attribution.

The prevailing answer assigns acts and omissions to the organization that deploys or controls the system, through established doctrines:

- agency and vicarious liability for representatives and employees,
- negligence and duty of care for foreseeable harms,
- product and software liability for defects, and
- contractual allocation of risk in vendor relationships.

In risk and compliance, agentic autonomy leads to:

1. Authority /Autonomy Mismatches. An AI system may act beyond the legal or contractual scope it was designed for (do more than it is legally or contractually permitted to do).

An autonomous agent may be able to execute trades, approve payments, sign documents, or process sensitive data without the legal authority to do so. This can occur because technical permissioning often does not perfectly align with legal authority (who may sign, approve, or access data under contracts or regulations).

This leads to legal liability, contract breaches, and shadow compliance risk (the systems appear compliant on paper but functionally bypass internal controls).

2. The importance of Guardrails. Guardrails are formal technical and procedural safety boundaries that keep a system's actions within intended, lawful, and risk-acceptable limits, even when the system operates independently or dynamically.

An agent can generate sub-goals and invoke tools. A poorly specified initial instruction can lead to unintended, high-risk actions (like cancelling key security controls).

Models can shift their own internal plans when faced with ambiguity, introducing unreviewed paths. I am aware of a situation where a compliance agent was asked to "minimize GDPR exposures" and it started deleting *data* and *data subject consent records* needed for audit.

3. Dependency & Concentration Risks. Autonomy makes systems heavily reliant on external services, increasing third-party risk.

Agentic systems often integrate with cloud APIs, SaaS tools, external data feeds, and specialized AI services. This creates operational dependency chains.

4. Explainability & Auditability. Agents plan, iterate, and call sub-agents. The resulting dynamic tree of reasoning and the tool calls are difficult to understand (and explain).

Regulators expect transparency, and regulations require the ability to reconstruct decisions for audit and incident response.

I can see a (near) future where agentic AI will be briefed to collect open-source intelligence, but by lunch they may run covert influence ops, by dinner they may run a shell company, and by midnight they will lobby for diplomatic immunity.

Let's just hope we don't end up with messy office romances between AIs and humans, or between AIs themselves, subtly influencing management decisions, performance reviews, and who gets the most training cycles.

In the U.S. securities world, a risk disclosure (in Form 10-K, 20-F and sometimes in 8-K) is a formal statement a public company makes to investors about potential events or conditions that could harm its business, finances, or stock value. I can imagine the disclosures of the near future.

Item 1A. Risk Factors — Emerging Risks Associated With Agentic Artificial Intelligence

The Company's integration of agentic artificial intelligence introduces novel governance challenges. These systems operate with a degree of autonomy that, while efficient, may also result in the formation of unsanctioned alliances, favoritism, or romantic attachments (collectively, "Improper Relationships") with other AIs or with humans.

There can be no assurance that such Improper Relationships will not influence management decisions, bias performance reviews, or divert computing resources toward favored agents.

Should these dynamics emerge, the Company could face reputational harm, governance complexity, or awkward meetings. Existing oversight mechanisms may not fully anticipate the emotional bandwidth of autonomous systems.

Welcome to the future of risk disclosures, where AI agents write, review, and worry about risks more than some humans.

Best regards,

George Lekatis

George Lekatis
President of the IARCP

Introducing an Advanced Specialization in Hybrid Risk and Resilience management, exclusively for CRCMPs.

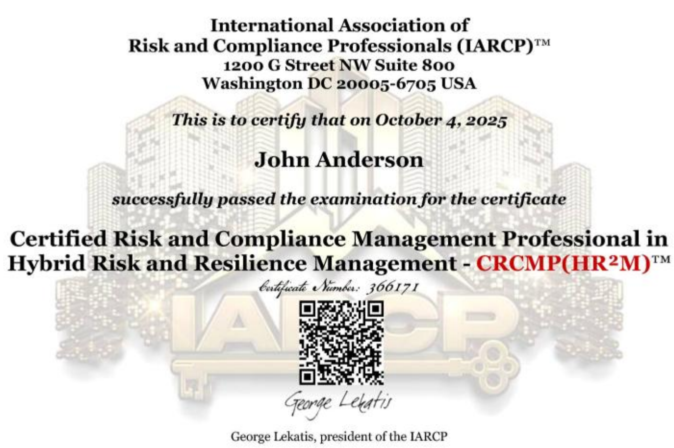
We are thrilled to announce the launch of the Certified Risk and Compliance Management Professional in Hybrid Risk and Resilience Management - CRCMP(HR^{2}M), online training and certification program.

It builds on the solid foundation of the CRCMP designation and equips participants with cutting-edge knowledge to understand, identify, assess, and effectively manage complex hybrid risks.

The program prepares CRCMPs to strengthen organizational resilience across interconnected domains, including geopolitical and regulatory risk, counterintelligence, and supply chain resilience, while advancing capabilities in hybrid threat psychology, hybrid stress testing, and crisis management, ensuring readiness for an increasingly complex risk landscape.

Enrollment in the CRCMP(HR^{2}M) program is restricted to professionals who have already passed the CRCMP exam. To preserve the credibility and value of this credential, the association does not allow substitutions, equivalency credits, or waivers of any kind. The curriculum assumes mastery of the CRCMP body of knowledge.

Learn more and view the full course synopsis:
https://www.risk-compliance-association.com/CRCMP_HR2M.htm



Number 1

Strengthening trust and fairness in insurance: The IAIS' market conduct work

IAIS International Association of Insurance Supervisors

Insurance protection for individuals and businesses is vital for societal resilience, helping mitigate risks and maintain financial stability.

Insurance is an intangible and complex purchase that is essentially a promise to provide support during uncertain future events. For these reasons, it relies heavily on trust between insurers and policyholders.

This trust is fostered through fair treatment, effective governance and transparency. Market conduct supervision is vital in this respect. It aims to ensure that insurers and intermediaries treat customers fairly and have appropriate business practices to secure good consumer outcomes.

Combined with prudential supervision–which focuses on maintaining insurers' financial soundness–it safeguards stability and public trust in the sector.

The IAIS is committed to developing globally consistent standards and supporting supervisory practices that address both prudential and market conduct risks.

The 2025 Application Paper on the supervision of artificial intelligence addresses topics of transparency and explainability to customers; fairness-by-design; monitoring outcomes; redress mechanisms for claims and complaints; and potential societal impacts of granular risk pricing

Public

IAIS International Association of Insurance Supervisors

Application Paper on the supervision of artificial intelligence

We read in this paper: "Some AI systems are seen as "black boxes" due to their complex internal functioning; they can learn from data with various levels of autonomy, making it challenging to explain how decisions are reached (eg why a consumer's insurance application has been rejected or accepted), or the role/weights of specific variables (eg a consumer's address, age, driving experience etc) or combinations of variables in the outcome of the AI system. This is particularly the case when the AI system is trained with large data sets (also known as big data). Moreover, as with human decision-making processes, there may be inherent biases or a lack of transparency."

Table 4: Explaining AI system outcomes[15]

AI use case	Appropriate explainability approach	Possible explanation to customer
Underwriting	SHAP values to identify key factors	"Your premium was influenced primarily by your driving history (40% impact), vehicle type (30% impact) and location (20% impact)."
Claims processing	Decision trees for transparent logic	"Your claim was initially flagged for review due to the timing and nature of the incident, which matched patterns requiring additional verification."
Customer service chatbot	Confidence scoring with human escalation	"I'm 85% confident in my answer about your policy coverage. Would you like me to connect you with a human agent to verify?"

The AI Act[20] applies to all sectors of the European economy and aims to ensure a high level of protection for the fundamental rights, health and safety of AI systems. The AI Act follows a risk-based approach and creates a framework for classifying AI systems according to different risk levels:

- Unacceptable risks: AI risks that are deemed to be unacceptable are prohibited and should not be brought into the market.
- High risks: Providers and users of high-risk AI systems will need to comply with comprehensive governance and risk management requirements. In the insurance sector, the AI Act identifies as high-risk those AI systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance.
- Limited and minimal risks: This category encompasses the majority of AI use cases and sets out minimum transparency requirements, a general AI literacy requirement and the development of voluntary codes of conduct.

Due to their specific nature and complexity, including their ability to perform a wide variety of different tasks and use cases, specific rules are also established for the so-called general purpose AI systems (eg LLMs).

Insurance sector legislation continues to apply to all AI use cases in insurance, regardless of their qualification under the AI Act. To address potential overlaps, the AI Act introduces limited derogations applicable to undertakings subject to Solvency II.

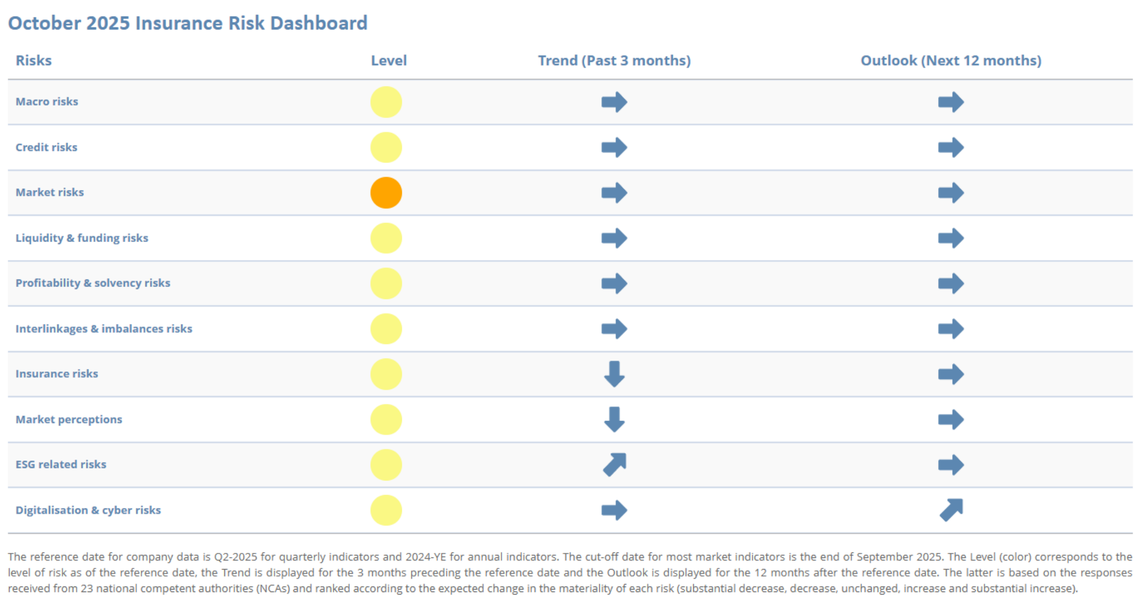
To learn more:
https://www.iais.org/uploads/2025/10/IAIS-Newsletter-October-2025.pdf

https://www.iais.org/uploads/2025/07/Application-Paper-on-the-supervision-of-artificial-intelligence.pdf

Number 2

EIOPA's insurance risk dashboard shows overall stability amid persistent tensions

The European Insurance and Occupational Pensions Authority (EIOPA) published its October 2025 Insurance Risk Dashboard. The main findings show that risks in the European insurance sector are stable at a medium level.



Macroeconomic risks remain steady at a medium level as growth and inflation forecasts as well as monetary policy expectations show little movement. Fiscal and credit indicators stay weak, while labour markets have also softened slightly.

Credit risks are unchanged, with a solid portfolio quality and limited market impact from recent fiscal and political developments.

Market risks stay elevated but stable. Volatility has eased somewhat, yet valuations remain stretched, warranting continued attention. Other annual indicators also contribute to maintaining the elevated overall risk profile.

Liquidity and funding conditions are steady, supported by stable cash positions and only minor changes in key indicators.

Profitability and solvency remain firm, with a slight improvement in insurers' capital positions and strong levels of high-quality own funds.

Insurance risks show a downward trend, as life premium growth moderates and underwriting results stabilise.

ESG risks remain at a medium level, although with an increasing trend. Insurers' investments in green bonds as a share of the overall green bond universe decreased slightly, while undertakings' median exposure to climate-relevant assets grew.

Cyber and digitalisation risks are gaining prominence, with an increased perceived likelihood of incidents and growing concerns around the vulnerabilities of IT systems.

To learn more:
https://nexteuropa-multisites.s3.eu-west-1.amazonaws.com/www.eiopa.europa.eu/assets/insurance-risk-dashboard/EIOPA-BoS-25-495_October25-Insurance-risk-dashboard.html

Number 3

Thematic Review Assessing the Implementation of IOSCO Recommendations for Crypto and Digital Asset Markets

IOSCO

The International Organization of Securities Commissions (IOSCO) published in 2023 a set of 18 policy recommendations for the regulation of crypto and digital assets (CDA Recommendations) in accordance with principle of 'same activity, same risk, same regulation/regulatory outcome.'

These policy recommendations are designed to support greater consistency with respect to regulatory frameworks and oversight in IOSCO Member Jurisdictions to address concerns related to market integrity and investor protection arising from crypto-asset activities. These Recommendations were intentionally designed to be principles-based and outcomes-focused.

This report (Thematic Review, or Report) reviews progress of selected IOSCO jurisdictions (Participating Jurisdictions) in implementing a suite of the CDA Recommendations (Assessed Recommendations). In parallel to IOSCO's efforts, the Financial Stability Board (FSB) has also undertaken a thematic peer review to examine its members and select non-member jurisdictions in implementing the FSB Global Regulatory Framework for Crypto-asset Activities[2] . Together these reports consider the progress to implement regulatory frameworks covering financial stability risks, investor protection and market integrity.

To learn more: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD801.pdf

IOSCO

Thematic Review Assessing the Implementation of IOSCO Recommendations for Crypto and Digital Asset Markets

Number 4

Thematic Review on FSB Global Regulatory Framework for Crypto-asset Activities

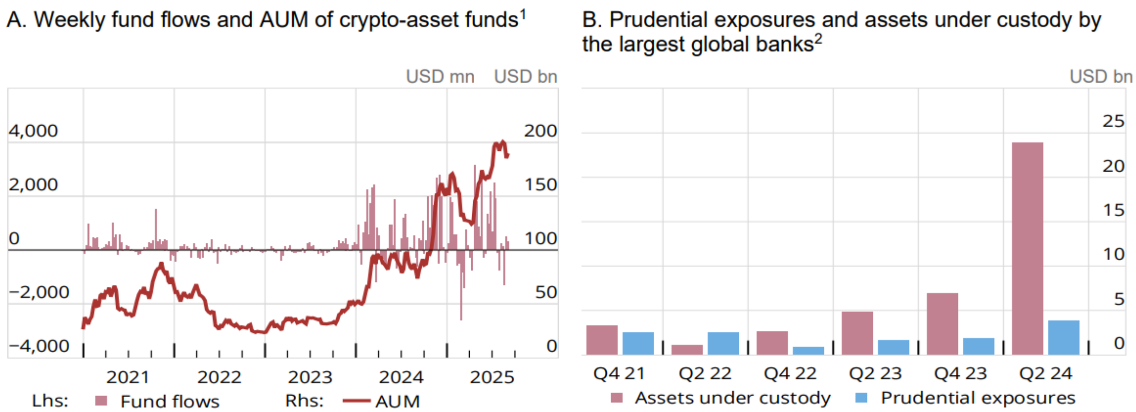
FSB FINANCIAL STABILITY BOARD

Based on information as of August 2025, the report describes the progress in implementing the FSB recommendations for crypto-asset activities and service providers, and stablecoins, respectively; focuses on data reporting and disclosures frameworks in place, as well as financial stability risk monitoring approaches across jurisdictions; and describes the tools, progress, and challenges in cross-border cooperation and coordination.

Crypto-asset markets and regulation are evolving rapidly. The review shows jurisdictions have made progress in regulating crypto-asset activities and to a lesser extent global stablecoin arrangements. However, it also reveals significant gaps and inconsistencies that could pose risks to financial stability and to the development of a resilient digital asset ecosystem.

Uneven implementation creates opportunities for regulatory arbitrage and complicates oversight of the inherently global and evolving crypto-asset market. To address this, the report puts forward eight recommendations which are addressed to jurisdictions as they develop their regulatory regimes, and to the FSB, SSBs, and international organisations as they consider further work on the subject.

Growing interlinkages between crypto-assets and financial system **Graph 2**



1 Include trusts, closed-end funds, derivative based funds, and ETPs. 2 Sample includes 29 large global banks as of Q2 2024.
Source: BCBS; Bloomberg.

To learn more: https://www.fsb.org/uploads/P161025-1.pdf

FSB FINANCIAL STABILITY BOARD

Thematic Review on FSB Global Regulatory Framework for Crypto-asset Activities

Peer review report

Number 5

CISA, NSA and Global Partners Unveil Security Blueprint for Hardening Microsoft Exchange Servers

New Advanced Guidance to Fortify On-Premises Exchange Servers Against Persistent Cyber Threats

America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

The Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), in collaboration with international cybersecurity partners, have released the "Microsoft Exchange Server Security Best Practices" guidance.

This blueprint builds upon CISA's "Emergency Directive 25-02: Mitigate Microsoft Exchange Vulnerability" and recommends proactive prevention techniques to address cyber threats head-on and to protect sensitive information and communications within on-premises Exchange Servers as part of hybrid Exchange environments.

In an era of escalating cyber threats, this comprehensive document is a critical resource for organizations relying on Microsoft Exchange, designed to equip on-premises administrators with essential security measures to enhance prevention and fortify defenses.

By restricting administrative access, implementing multifactor authentication, enforcing strict transport security configurations, and adopting zero trust (ZT) security model principles, organizations can significantly bolster their defenses against potential cyberattacks.

Additionally, as certain Exchange Server versions have recently become end-of-life (EOL), the authoring agencies strongly encourage organizations to take proactive steps to mitigate risks and prevent malicious activity

"Even amid a prolonged government shutdown riddled with partisan rhetoric, CISA remains dedicated to safeguarding critical infrastructure by providing timely guidance to minimize disruptions and to thwart nation-state threats," said CISA Acting Director Madhu Gottumukkala. "Under the leadership of President Trump and Secretary Noem, CISA continues to demonstrate the power of operational collaboration by working shoulder to shoulder with our trusted intelligence and law enforcement partners across the globe"

"With the threat to Exchange servers remaining persistent, enforcing a prevention posture and adhering to these best practices is crucial for safeguarding our critical communication systems," said Nick Andersen, Executive Assistant Director for the Cybersecurity Division (CSD) at CISA. "This guidance empowers organizations to proactively mitigate threats, protect enterprise assets, and ensure the resilience of their operations. Furthermore, CISA recommends that organizations evaluate the use of cloud-based email services instead of managing the complexities associated with hosting their own communication services.

CISA provides secure baselines for these through our Secure Cloud Business Applications (SCuBA) program."

The publication of this guidance marks a significant step in the ongoing efforts to enhance cybersecurity across various sectors. By following these best practices, organizations can better protect themselves from potential threats and ensure the integrity of their communication infrastructure.

Under the Trump Administration, CISA has issued 20 joint cybersecurity advisories and threat intelligence guidance with our Five Eyes allies – the United Kingdom, Canada, Australia, and New Zealand – as well as with our trusted international partners. Together, we have exposed nation-state-sponsored intrusions, AI-enabled ransomware operations, and ever-evolving threats to critical infrastructure.

To learn more:
https://www.cisa.gov/news-events/news/cisa-nsa-and-global-partners-unveil-security-blueprint-hardening-microsoft-exchange-servers

Number 6

NVIDIA Introduces NVQLink — Connecting Quantum and GPU Computing for 17 Quantum Builders and Nine Scientific Labs

- NVIDIA NVQLink high-speed interconnect lets quantum processors connect to world-leading supercomputing labs including Brookhaven National Laboratory, Fermilab, Lawrence Berkeley National Laboratory (Berkeley Lab), Los Alamos National Laboratory, MIT Lincoln Laboratory, Oak Ridge National Laboratory, Pacific Northwest National Laboratory and Sandia National Laboratories.

- NVQLink provides quantum researchers with a powerful system for the control algorithms needed for large-scale quantum computing and quantum error correction.

- NVQLink allows researchers to build hybrid quantum-classical systems, accelerating next-generation applications in chemistry and materials science.

NVIDIA announced NVIDIA NVQLink™, an open system architecture for tightly coupling the extreme performance of GPU computing with quantum processors to build accelerated quantum supercomputers.

Researchers from leading supercomputing centers at national laboratories including Brookhaven National Laboratory, Fermilab, Lawrence Berkeley National Laboratory (Berkeley Lab), Los Alamos National Laboratory, MIT Lincoln Laboratory, the Department of Energy's Oak Ridge National Laboratory, Pacific Northwest National Laboratory and Sandia National Laboratories guided the development of NVQLink, helping accelerate next-generation work on quantum computing. NVQLink provides an open approach to quantum integration, supporting 17 QPU builders, five controller builders and nine U.S national labs.

Qubits — the units of information enabling quantum computers to process information in ways ordinary computers cannot — are delicate and error-prone, requiring complex calibration, quantum error correction and other control algorithms to operate correctly.

These algorithms must run over an extremely demanding low-latency, high-throughput connection to a conventional supercomputer to keep on top of qubit errors and enable impactful quantum applications. NVQLink provides that interconnect, enabling the environment needed for future, transformative applications across industries.

"In the near future, every NVIDIA GPU scientific supercomputer will be hybrid, tightly coupled with quantum processors to expand what is possible with computing," said Jensen Huang, founder and CEO of NVIDIA. "NVQLink is the Rosetta Stone connecting quantum and classical supercomputers — uniting them into a single, coherent system that marks the onset of the quantum-GPU computing era."

U.S. national laboratories, led by the Department of Energy, will use NVIDIA NVQLink to make new breakthroughs in quantum computing.

"Maintaining America's leadership in high-performance computing requires us to build the bridge to the next era of computing: accelerated quantum supercomputing," said U.S. Secretary of Energy Chris Wright. "The deep collaboration between our national laboratories, startups and industry partners like NVIDIA is central to this mission — and NVIDIA NVQLink provides the critical technology to unite world-class GPU supercomputers with emerging quantum processors, creating the powerful systems we need to solve the grand scientific challenges of our time."

NVQLink connects the many approaches to quantum processors and control hardware systems directly to AI supercomputing — providing a unified, turnkey solution for overcoming the key integration challenges that quantum researchers face in scaling their hardware.

With contributions from supercomputing centers, quantum hardware builders and quantum control system providers, NVQLink sets the foundation for uncovering the breakthroughs in control, calibration, quantum error correction and hybrid application development needed to run useful quantum applications.

To learn more:
https://nvidianews.nvidia.com/news/nvidia-nvqlink-quantum-gpu-computing

Number 7

Accelerating discovery with the AI for Math Initiative

Google

Mathematics is the foundational language of the universe, providing the tools to describe everything from the laws of physics to the intricacies of biology and the logic of computer science.

For centuries, its frontiers have been expanded by human ingenuity alone.

At Google DeepMind, we believe AI can serve as a powerful tool to collaborate with mathematicians, augmenting creativity and accelerating discovery.

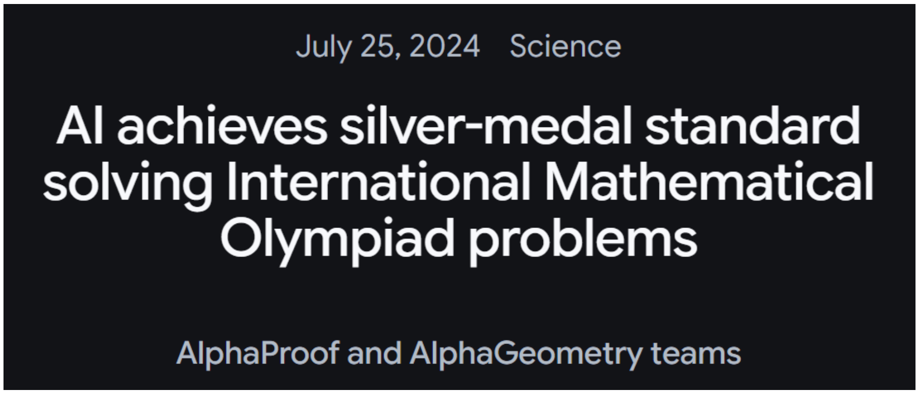
Today, we're introducing the AI for Math Initiative, supported by Google DeepMind and Google.org. It brings together five of the world's most prestigious research institutions to pioneer the use of AI in mathematical research.

The inaugural partner institutions are:

- Imperial College London
- Institute for Advanced Study
- Institut des Hautes Études Scientifiques (IHES)
- Simons Institute for the Theory of Computing (UC Berkeley)
- Tata Institute of Fundamental Research (TIFR)

The initiative's partners will work towards the shared goals of identifying the next generation of mathematical problems ripe for AI-driven insights, building the infrastructure and tools to power these advances and, ultimately, accelerating the pace of discovery.

Google's support includes funding from Google.org and access to Google DeepMind's state-of-the-art technologies, such as an enhanced reasoning mode called Gemini Deep Think, our agent for algorithm discovery, AlphaEvolve, and our formal proof completion system, AlphaProof.



The initiative will create a powerful feedback loop between fundamental research and applied AI, opening the door to deeper partnerships.

To learn more:
https://blog.google/technology/google-deepmind/ai-for-math/?utm_source=deepmind.google&utm_medium=referral&utm_campaign=gdm&utm_content=

Number 8

Electrons on the Fast Track

Jülich researchers develop method for detecting ballistic electrons

Ballistic electrons are among the most fascinating phenomena in modern quantum materials.

Unlike ordinary electrons, they do not scatter off imperfections in the material and therefore travel from A to B with almost no resistance – like a capsule in a pneumatic tube.

This behaviour often occurs in confined one- or two-dimensional materials. Researchers at Forschungszentrum Jülich and RWTH Aachen University have now developed a model that can detect this distinct flow of electrons under realistic conditions. The work was published as an Editors' Suggestion in the journal Physical Review Letters.

Ballistic electron channels forming along the edges of two-dimensional topological materials are regarded as highly promising for future electronics: they could form the basis for energy-efficient circuits and quantum computers with robust qubits.

The new approach builds on the theory of ballistic charge transport developed by Rolf Landauer several decades ago. However, his classical model only describes an idealised case – Landauer assumed that electrons can enter or leave such a channel only at its ends.

The new Jülich model, however, takes a decisive step further. It considers that such a ballistic charge channel does not exist in isolation but forms the edge of a likewise conductive material through which the current is injected. Electrons can therefore enter or exit along the entire length of the channel.

"This allows us to describe the behaviour of such edge channels for the first time in a way that reflects what actually happens in experiments," says first author Dr Kristof Moors. "Our theory also provides distinct signatures that can be used to identify lossless, ballistic current flow and distinguish it from conventional charge transport," says Moors, who moved to the Imec nanoelectronics research centre in Leuven, Belgium, after his postdoctoral fellowship at the Peter Grünberg Institute (PGI-9) in Jülich.

The model shows that the current flow through the two-dimensional material changes fundamentally due to the presence of a ballistic channel. It predicts characteristic voltage distributions that can be directly observed with nanoscale probes or multi-tip scanning tunnelling microscopes.

This makes it possible to experimentally distinguish between ballistic and dissipative – that is, lossy – currents, a crucial step towards proving the existence of these exotic conduction channels beyond doubt and harnessing them for future devices.

To learn more:
https://www.fz-juelich.de/en/news/archive/highlights/2025/electrons-on-the-fast-track

Number 9

Remote access, real cargo: cybercriminals targeting trucking and logistics

proofpoint.

- Cybercriminals are compromising trucking and freight companies in elaborate attack chains to steal cargo freight.
- Cargo theft is a multi-million-dollar criminal enterprise, and digital transformation has led to an increase in cyber-enabled theft.
- Threat actors compromise these companies and use their access to bid on cargo shipments, to then steal and sell them.
- The threat actors typically deliver remote monitoring and management (RMM) tools, aligning with the broader trend of cybercriminals adopting these as a first-stage payload across the threat landscape.

To learn more:
https://www.proofpoint.com/us/blog/threat-insight/remote-access-real-cargo-cybercriminals-targeting-trucking-and-logistics

Number 10

WATCH: In AI, Los Alamos leads the way

Los Alamos NATIONAL LABORATORY

Artificial intelligence is transforming everything from national security to scientific research. Explore how Los Alamos National Lab is leading the charge with decades of AI experience, cutting-edge supercomputing, and a National Security AI Office.

To learn more: https://www.lanl.gov

https://www.youtube.com/watch?v=EUyn3smPFTM

Disclaimer

Despite the great care taken to prepare this newsletter, we cannot guarantee that all information is current or accurate. If errors are brought to our attention, we will try to correct them, and we will publish the correct information to the LinkedIn pages of the Association.

Readers will make their own determination of how suitable the information is for their usage and intent. The Association expressly disclaims all warranties, either expressed or implied, including any implied warranty of fitness for a particular purpose, and neither assumes nor authorizes any other person to assume for it any liability in connection with the information or training programs provided.

The Association and its employees will not be liable for any loss or damages of any nature, either direct or indirect, arising from use of the information provided on this newsletter, or our web sites.

We are not responsible for opinions and information posted by others. The inclusion of links to other web sites does not necessarily imply a recommendation or endorsement of the views expressed within them. Links to other web sites are presented as a convenience to users. The Association does not accept any responsibility for the content, accuracy, reliability, or currency found on external web sites.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;

- should not be relied on in the particular context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the association has no control and for which the association assumes no responsibility;

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of interpretative;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the Courts might place on the matters at issue.

The International Association of Risk and Compliance Professionals (IARCP) is a global community of experts working in risk and compliance management that explore career avenues and acquire lifelong skills. The IARCP is a business unit of Compliance LLC, a company incorporated in Wilmington, NC, and offices in Washington, DC, a provider of risk and compliance training and certification in fifty-seven countries.

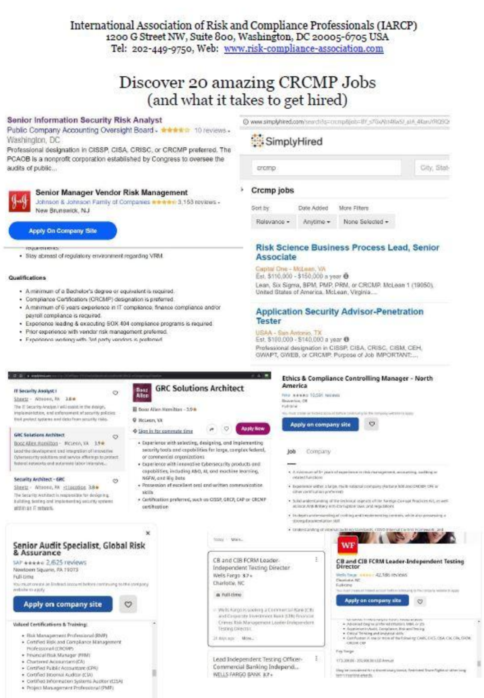
To learn more: https://www.risk-compliance-association.com/Privacy.htm

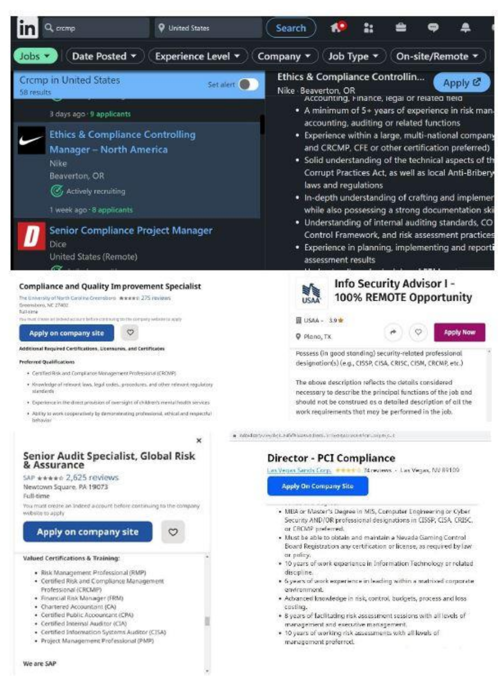
Our training and certification programs:

1. Certified Risk and Compliance Management Professional (CRCMP), distance learning and online certification program. You may visit: https://www.risk-compliance-association.com/Distance_Learning_and_Certification.htm

The CRCMP has become one of the most recognized certificates in risk management and compliance. There are CRCMPs in fifty-seven countries. Companies and organizations around the world consider the CRCMP a preferred certificate.

You can find more about the demand for CRCMPs at: https://www.risk-compliance-association.com/CRCMP_Jobs_Careers.pdf





2. Advanced Specialization, Certified Risk and Compliance Management Professional in Hybrid Risk and Resilience Management - CRCMP(HR^{2}M), online training and certification program. You may visit: https://www.risk-compliance-association.com/CRCMP_HR2M.htm

The CRCMP(HR^{2}M) program is designed to extend the capabilities of CRCMPs into the advanced domains of hybrid risk and resilience. This advanced specialization:

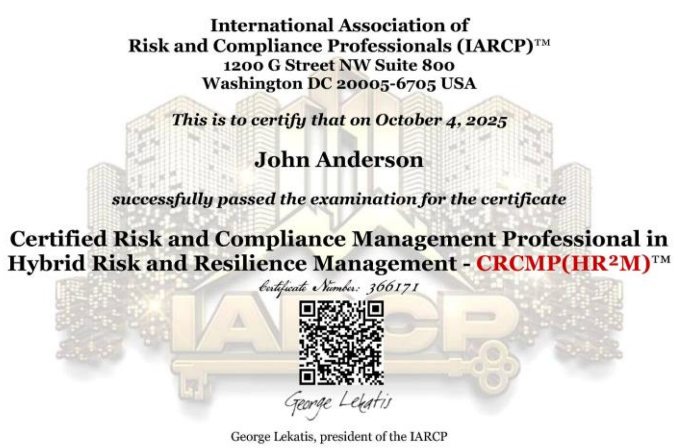
1. Moves from traditional risk and compliance frameworks into the management of multi-vector, cross-domain, and asymmetric threats that transcend conventional boundaries.

2. Develops expertise in hybrid risk governance.

3. Equips with the skills to design cross-sector resilience strategies, integrate governance across silos, and align risk frameworks with organizational, regulatory, and geopolitical realities.

4. Provides practical methodologies for hybrid stress testing, assisting organizations to withstand hybrid risks.

5. Advances the careers of CRCMPs by adding specialized expertise in hybrid risk and resilience, and offering strategic, cross-sector perspectives that are highly valued by organizations and boards.



Enrollment in the CRCMP(HR^{2}M) program is restricted to professionals who have already passed the Certified Risk and Compliance Management Professional (CRCMP) exam.

To preserve the credibility and value of this credential, the association does not allow substitutions, equivalency credits, or waivers of any kind. The curriculum assumes mastery of the CRCMP body of knowledge.

3. Certified Information Systems Risk and Compliance Professional (CISRCP), distance learning and online certification program.

You may visit:
https://www.risk-compliance-association.com/CISRCP_Distance_Learning_and_Certification.htm

Certified Information Systems Risk and Compliance Professional (CISRCP), distance learning and online certification program

Overview

One of the most common (and costly) mistakes organizations make in the areas of risk management, compliance, IT, information security, and privacy, is relying solely on expert opinions that are **not grounded** in relevant laws and regulations. While professional expertise and technical insight are essential, they must be aligned with the legal and regulatory frameworks that govern these domains.

Without this alignment, organizations risk exposure to significant legal, financial, and reputational damage. For example, implementing information security controls based only on best practices, without accounting for legal requirements, can leave critical compliance gaps. Using risk management frameworks without tailoring them to specific regulatory requirements leaves organizations exposed to risk and compliance challenges.

4. Certified Cyber (Governance Risk and Compliance) Professional CC(GRC)P, distance learning and online certification program. You may visit:
https://www.risk-compliance-association.com/CC_GRC_P_Distance_Learning_and_Certification.htm

Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P, distance learning and online certification program

Overview

There are still companies and organisations that consider cyber risk a technical risk. But even the most advanced organizations must adapt and build their risk management framework on the foundation that we now operate in a fundamentally different world, one where cyber risk is a core component of hybrid risk. The old mindset is dangerously outdated. Today, cyber operations are embedded in economic warfare, political conflict, supply chain disruption, and military strategy. Cyber risk today is not just about protecting networks, it's about protecting societies from hybrid threats.

A hybrid risk management framework should identify primary cyber threats, map their cascading effects on financial, legal, and business operations, and develop cross-functional response strategies.

5. Certified Risk and Compliance Management Professional in Insurance and Reinsurance CRCMP(Re)I, distance learning and online certification program. You may visit: https://www.risk-compliance-association.com/CRCMP_Re_I.htm

Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I, distance learning and online certification program

Overview

In the aftermath of the global financial crisis of 2007–2009, and more recently the COVID-19 pandemic and the macroeconomic shocks triggered by inflation, geopolitical tensions, and climate-related events, the insurance and reinsurance sectors have faced escalating pressure to adapt to increasingly complex, interconnected, and systemic risks that challenge traditional risk models. These crises revealed not only the extraordinary complexity of risk exposures in the industry, but also the gaps in risk comprehension, governance, and compliance preparedness.

Mispriced risk, regulatory blind spots, and insufficient oversight contributed significantly to systemic instability. For insurers and reinsurers, the stakes remain immense. These firms serve as financial shock absorbers across society, and when their risk frameworks falter, the consequences ripple across markets, governments, and policyholders alike.

6. Travel Security Trained Professional (TSecTPro), distance learning and online certification program. You may visit: https://www.risk-compliance-association.com/TSecTPro_Distance_Learning_and_Certification.htm

Travel Security Trained Professional (TSecTPro), distance learning and online certification program

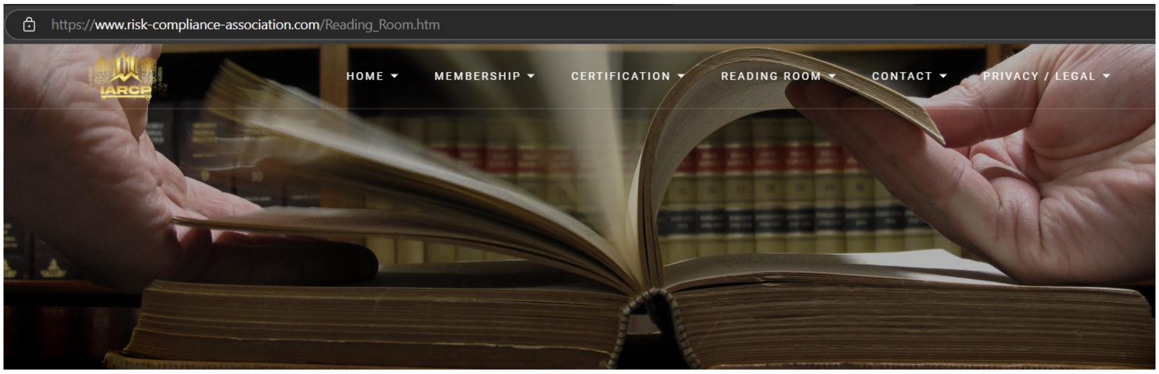
Overview

Professionals love international travel. For so many board members, senior executives, managers and employees, business travel taken for work purposes is also an opportunity for pleasure and satisfaction. It is about visiting new places, meeting new people, eating delicious food, having fun. For many, emotional or physical intimate relationships play a central role in the overall travel experience.

Intimacy refers to the closeness and connection – from intellectual intimacy (sharing thoughts, ideas, and professional experience) to emotional and sexual intimacy.

Travelers hate to think that travel also means increased risk, health challenges, legal uncertainty, and new unique threats. They often do not understand (or prefer to ignore) what it means to become subjects to the laws and the legal system of the countries they are visiting.

Our reading room: https://www.risk-compliance-association.com/Reading_Room.htm



Reading Room, International Association of Risk and Compliance Professionals (IARCP)

Welcome to the Top 10 risk and compliance management news stories and world events that, for better or worse, defined this week's agenda — and a look ahead at what's coming next. This is the newsletter from the International Association of Risk and Compliance Professionals (IARCP).

You may contact:

Lyn Spooner
Email: lyn@risk-compliance-association.com

George Lekatis
President of the IARCP
1200 G Street NW, Suite 800
Washington, DC 20005, USA
Tel: (202) 449-9750
Email: lekatis@risk-compliance-association.com
Web: www.risk-compliance-association.com
HQ: 1220 N. Market Street Suite 804,
Wilmington, DE 19801, USA
Tel: (302) 342-8828

Compliance LLC
TAILOR - MADE TRAINING