Monday, January 5, 2026

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.

Santa and his elves were working happily in the North Pole. They made toys, wrapped presents, and kept the Nice List (who gets presents) and the Naughty List (who didn't behave) safe in a very special environment, the Gift Network.

One morning, jingle bells suddenly turned into warning bells. Santa's screen flashed: ALERT: Unauthorized access to the Nice List.

Santa gathered his Cyber Elves, a remarkable team of specialists who work tirelessly behind the scenes at the North Pole to protect the magic of Christmas. Each elf has a playful title that makes children smile but also has a critical role in cybersecurity and hybrid resilience.

The elves discovered that a sneaky group called the Frostbyte Federation was trying to hack Christmas. So, what do they try to achieve? More presents?

According to Sneakerton Snowpsy, Santa's Chief Counter Elf Intelligence Officer, Frostbyte Federation is a state sponsored hybrid threat actor. Whenever Santa asks if Sneakerton obtained classified warnings from the NSA, he responds: "No Such Agency." The other elves exchange puzzled looks, because they all know that the North Pole's intelligence budget is mostly spent on GPS maintenance.

Ordinary cybercriminals have simple and self centered goals. They want extra presents, more candy canes than their ratings allow (from the Santa Rating Agency), and a way to sneak names from the Naughty List to the Nice List without learning any lessons about kindness.

A state sponsored group would pursue entirely different objectives. They would be acting to benefit a powerful patron, a rival holiday authority, even a jealous force that envies Santa's global influence.

Their objective would shift from personal advantage to strategic disruption. Instead of stealing toys for themselves, they might seek to destroy the world's confidence in Santa's ability to deliver joy. They would try to spark doubt and disappointment across continents. If a state backed adversary could disrupt Santa's perfectly timed logistics system, it would be a triumph for him.

State sponsored agents could alter millions of entries worldwide, triggering blame, chaos, and distrust. A child who behaved beautifully all year but receives nothing becomes a loud voice of complaint. Multiply that by many thousands and suddenly Christmas begins to look unfair or broken.

Motivation shapes patience. A criminal wants a fast win. A state sponsored faction would embed silently in Santa's networks for months, waiting for the exact moment when their interference would have the most devastating emotional impact. They would measure success in collapsed trust, and widespread holiday disillusionment. In the criminal scenario, the target is Santa's treasure. In the state sponsored scenario, the target is Santa's legacy.

A new trouble begins with whispers that creep into the morning light, spread by several social media accounts. A carefully crafted disinformation campaign has taken root around Santa's operations. At first there are posts claiming Santa prefers children from one village over another, and in a short clip, Santa is angrily refusing to deliver gifts to an entire town. Rumors spread across the internet, amplified by automated bots that exaggerate every complaint.

The campaign is clever enough, and many believe it. Parents post outraged messages, newspapers pick up the story, and children begin to worry that Santa has changed.

Then we have some inside information, from Blinky Truthbell, an anxious little elf with glasses too big for his face. He discloses that many toys were placed under quality review, and 24.3% of Santa's toys were proven dangerously defective. (Later, he accepted he was blackmailed! Adversaries had found unapproved tutorials on calligraphy in his laptop folder "*Accounting 2019*". They threatened to disclose to Santa what has happened.)

Parents around the world are now in panic mode. Complaints rise, and legitimate toy inspection teams must respond. In the EU, parents and social groups demand inspection of the Santa framework and ask for evidence about compliance with Directive 2009/48/EC on the safety of toys (the Toy Safety

Directive, this is not a joke), adopted by the European Parliament and the Council of the European Union on 18 June 2009.

Of course, the cybersecurity elves worked hard, and they announced something that included something like the phrase we detected anomalous cookie behavior on Port 443!

Within seconds, the parents' panic is obvious in the social media. Some are looking for the Port 443 shopping mall. The cybersecurity elves respond immediately. "No, no, it's not a port with boats, it's a port with network packets." It did not help at all. Santa must learn after the crisis that IT is not the most suitable team to communicate what has happened.

In the end, the North Pole survived, and the day was saved. The North Pole learned that modern crises do not respect anything. Disinformation can spread fast, morale can collapse quickly, and if leadership cannot communicate clearly, even the safest place on Earth can feel dangerously uncertain.

Santa concluded his after action report with a message. "We must defend not only our networks, but also our Christmas spirit. Because joy and trust are strategic assets. Adversaries will always try to break everything that unites us. If hybrid threats return, the North Pole will be ready, vigilant, and full of cookies that behave properly online."

Best regards,

George Lekatis
President of the IARCP

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

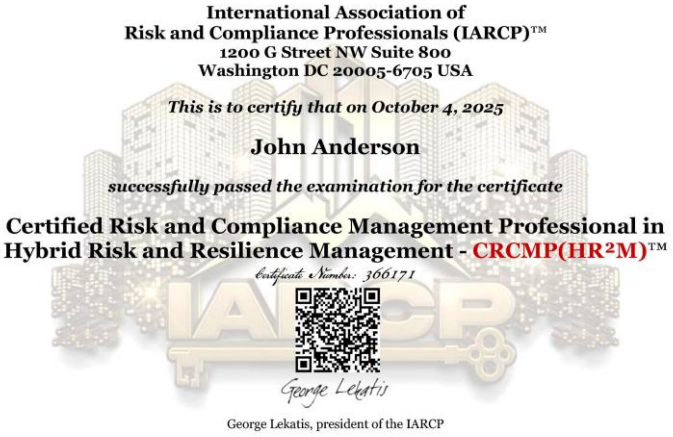
We are thrilled to announce the launch of the Certified Risk and Compliance Management Professional in Hybrid Risk and Resilience Management - CRCMP(HR²M), online training and certification program.

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(HR²M) 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 (Page 7)

Resilience

Remarks by Mr John C Williams, President and Chief Executive Officer of the Federal Reserve Bank of New York, at the New Jersey Bankers Association, Jersey City, New Jersey

Number 2 (Page 11)

Economic Resilience: What Next?

Gabriel Makhlouf, Governor of the Central Bank of Ireland, at The Royal Irish Academy, Dublin

Number 3 (Page 14)

EIOPA flags financial stability risks related to private credit, a weakening dollar and global interconnectedness

eiopa
European Insurance and Occupational Pensions Authority

Number 4 (Page 17)

The EBA provides guidance to banks on enhanced reporting requirements for operational risk ahead of new June 2026 reference date

eba European Banking Authority

Number 5 (Page 19)

Adverse scenarios for the 2025 European Insurance and Occupational Pensions Authority's EU-wide pension fund stress test exercise

ESRB
European Systemic Risk Board
European System of Financial Supervision

Number 6 (Page 22)

CISA Unveils Enhanced Cross-Sector Cybersecurity Performance Goals
New Benchmarks Empower Organizations to Counter Emerging Threats, Build Cyber Resilience, and Strengthen Governance

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

Number 7 (Page 25)

Call for Feedback: Advancing Software Supply Chain Security together!

enisa

Number 8 (Page 27)

Amazon Threat Intelligence identifies Russian cyber threat group targeting Western critical infrastructure

aws

Number 9 (Page 32)

The cyber threat to Canada's water systems: Assessment and mitigation

Government of Canada

Number 10 (Page 38)

The Cyber Defense Review - Resilient Dependencies: Preparing to Fight Through Cyber Disruption
Lt. Gen. Maria B. Barrett, U.S. Army Cyber Command, Fort Gordon, GA, USA

THE CYBER DEFENSE REVIEW

Number 1

Resilience

Remarks by Mr John C Williams, President and Chief Executive Officer of the Federal Reserve Bank of New York, at the New Jersey Bankers Association, Jersey City, New Jersey

Introduction

Good morning, everyone. It's great to be here at the Liberty Science Center, home of the largest planetarium in the Western Hemisphere. Typically, this would be the perfect opportunity for me to discuss the star variables in economics. Alas, I'll save that for the Q&A.

Instead, I'm going to talk to you today about the U.S. economy and how the Federal Reserve is working to achieve its dual mandate of maximum employment and price stability. I'll also discuss recent actions by the Federal Open Market Committee (FOMC), and I'll give my economic outlook.

Before I go further, I must give the standard Fed disclaimer that the views I express today are mine alone and do not necessarily reflect those of the FOMC or others in the Federal Reserve System.

Turning the Corner

One of the important parts of my job is to travel throughout the Federal Reserve's Second District. It gives me the opportunity to meet with business, community, and government leaders and get a firsthand and in-depth look at the challenges and opportunities facing our region.

In recent years, North Jersey has largely followed the trajectory of the broader U.S. economy: It was hit hard by the pandemic, rebounded quickly, grappled with inflation, and then, over the past year, faced heightened uncertainty stemming from geopolitical events and changes in trade policy.

In fact, if I had to choose one word to describe 2025, it is uncertainty. What's striking is that despite all the uncertainty, the U.S. economy has shown considerable resilience and looks poised to pick up steam next year.

In other words, after navigating through the challenges of 2025, we now appear to be turning the corner. Of course, there's always uncertainty about the road ahead—or, as we say in Jersey, about what's coming down the Turnpike. But over the past year, our local, national, and even global economies have proven to be resilient. Here, that resilience is called "Jersey Strong."

Temporarily Stalled

Before I talk about what I expect for the economy, I want to take a few minutes to tell you more about its current state. I'll focus on the two sides of the Fed's dual mandate: maximum employment and price stability.

I'll start with price stability, which the FOMC defines as 2 percent inflation1 over the longer run. In monetary policy, we rely on the totality of the data—and there is a lot of data. While we haven't had the normal flow of official data in recent months due to the government shutdown, we are able to use a wide array of indicators to monitor how the economy is doing.

What the data tell me is that the effects of trade policies have boosted inflation this year, but these effects have been more muted and drawn out than I originally anticipated. As a result of the tariffs, progress toward the FOMC's 2 percent longer-run inflation goal has temporarily stalled, with the most recent inflation reading of about 2-3/4 percent roughly unchanged from a year ago. While it is not possible to precisely measure the effects of trade policy actions, my estimate is that they have contributed around one half of a percentage point to the current inflation rate.

I do not see any signs of tariffs contributing to second-round or other spillover effects on inflation. In particular, no broad-based supply chain bottlenecks have emerged, shelter inflation has declined steadily, and measures of wage growth point to a continued gradual slowing. This is consistent with reports from around the Second District, where several of my business contacts have noted that, while tariffs continue to drive up their input costs, the pace of price increases has eased slightly.

Most importantly, inflation expectations remain well anchored. The New York Fed's Survey of Consumer Expectations (SCE) continues to show that inflation expectations remain well within their pre-Covid ranges. This is something I watch closely, because well-anchored expectations are critical to ensuring low and stable inflation.

Gradual Cooling

Turning to the employment side of our mandate, the data show that the labor market has continued to cool, with labor demand softening more than supply. Job growth has been anemic, and the unemployment rate has moved up steadily in recent months. These trends are also occurring in North Jersey, where we've seen slight declines in employment since January, and where many of our regional contacts, including those responding to our business surveys, are reporting job losses.

In addition, survey-based measures of the balance between demand and supply show increasing slack in the labor market. In the Conference Board's consumer confidence survey, a measure of the difference between the share of respondents who think jobs are plentiful and the share of those who think jobs are hard to get has declined throughout 2025. We have seen a similar pattern with the National

Federation of Independent Business's survey measure of the difficulty in filling jobs. And the SCE's "job security gap" measure—defined as respondents' job-finding expectations minus their job-loss expectations—has fallen considerably this year.

Many labor market indicators are now at levels we saw prior to the pandemic, a time when the market was not overheated. And although the labor market is clearly cooling, I should emphasize that this has been an ongoing, gradual process, without signs of a sharp rise in layoffs or other indications of rapid deterioration.

Monetary Policy and the Road Ahead

Looking ahead, it is imperative that we restore inflation to our 2 percent longer-run goal on a sustained basis. It is equally important to do so without creating undue risks to our maximum employment goal. My assessment is that in recent months, the downside risks to employment have increased as the labor market has cooled, while the upside risks to inflation have lessened somewhat.

Monetary policy is very focused on bringing these risks into balance. To that end, the FOMC has moved the modestly restrictive stance of monetary policy toward neutral. At its meeting last week, the FOMC decided to lower the target range for the federal funds rate by 1/4 percentage point to 3-1/2 to 3-3/4 percent. The accompanying FOMC statement said that "in considering the extent and timing of additional adjustments to the target range for the federal funds rate, the Committee will carefully assess incoming data, the evolving outlook, and the balance of risks." With these actions, monetary policy is well positioned as we head into 2026.

Looking ahead, I expect tariffs will have a largely one-off price level effect that will be fully realized in 2026. I anticipate inflation to decline to just under 2-1/2 percent next year before reaching the FOMC's longer-run 2 percent goal in 2027.

I expect real GDP growth to be about 2-1/4 percent in 2026, well above my forecast for this year's pace of around 1-1/2 percent. This pickup is in part due to the effects of the government shutdown, but it's also fueled by tailwinds from fiscal policy, favorable financial conditions, and increased investments in artificial intelligence.

And I expect the unemployment rate to rise to around 4-1/2 percent at the end of this year, reflecting some additional effects from the government shutdown. With my forecast of above-trend GDP growth, I expect the unemployment rate to gradually come down over the next few years.

Balance Sheet

Before I conclude, I'd like to briefly comment on the Fed's balance sheet. On December 1, the FOMC stopped reducing its holdings of Treasury securities and agency debt and agency mortgage-backed securities.4 With the level of bank reserves now deemed to be ample, the FOMC decided to initiate reserve

management purchases to maintain an ample level of reserves. This is the natural next step in the implementation of our ample reserves framework to ensure effective interest rate control.

With the steady decline in the level of reserves, we have observed upward pressure on repo rates at times in recent months. When this occurs, the Fed's standing repo operations can act as a shock absorber by capping pressures on money market rates resulting from strong liquidity demand or market stress. I fully expect that standing repo operations will continue to be actively used in this way.

Conclusion

So, after a year of uncertainty, we will be starting 2026 from a place of resilience. The economy is poised to return to solid growth and price stability.

But, as 2025 has shown, the road may shift in unpredictable ways. In assessing the future path of monetary policy, my views, as always, will be based on the evolution of the totality of the data, the economic outlook, and the balance of risks to the achievement of our maximum employment and price stability goals. We must be ready to adjust our route as needed to reach our destination.

You may visit:
https://www.newyorkfed.org/newsevents/speeches/2025/wil251215

Number 2

Economic Resilience: What Next?
Gabriel Makhlouf, Governor of the Central Bank of Ireland, at The Royal Irish Academy, Dublin

Good evening. Thank you for the invitation to join you today.

This evening I want to talk about economic resilience, what it is and whether we have enough of it. I spoke about economic resilience in my first speech as Governor – 6 years ago – and wrote to the Minister for Finance about it in early February this year. After everything that's happened since February, it feels timely to take stock of where we are. My conclusion is that we need to give it greater focus.

Let me start by setting out three propositions.

First, successful economies need a stable and sustainable macroeconomic framework, sound monetary policy that delivers stable and predictable prices, a prudent fiscal policy and debt that's under control. Successful economies are also characterised by well-regulated financial systems and well-functioning markets.

Second, change is a constant and economic resilience is, in essence, the ability of an economy to manage change, whether it is to withstand or recover from the effects of shocks, or the more gradual evolution to a different state.

Third, resilience is built, not granted, and requires constant investment in economic capital which consists of physical, human, social and natural capital. Those four components generate flows of tangible and intangible benefits that build resilience. Ultimately, the growth and distribution of our economic capital – and the ensuing resilience – support societies to prosper and generate longer-term or intergenerational wellbeing.

A snapshot of Ireland's economy today paints a positive picture. The last set of Central Bank projections back in September – the next set are due next week – described an economy growing steadily with employment up 2.3 per cent in the year to Q3 2025 and with unemployment remaining low.

The State's books are in good order: the Government's Budget forecast a headline surplus of 3 per cent with debt at 62 per cent of modified national income (GNI*). The latest Exchequer returns point to continued strong growth in tax receipts, fuelled in particular by corporation tax.

In fact, The Economist has just ranked Ireland as one of the world's best performing economies this year.

But of course a snapshot is just that. What matters is the bigger picture, and the horizon. That is somewhat cloudy, and somewhat worrying.

Major global policy shifts this year have added to the economic uncertainty which came from Russia's war in Ukraine, geopolitical tensions more generally and the slow but growing fragmentation of the global economy over the past decade. And closer to home, you won't be surprised to hear me say that Ireland is over-reliant on corporation tax – and from a small number of firms – which this year is set to account for one third of overall Exchequer revenue.

Uncertainty is not a new phenomenon, and history teaches us that periods of change are the norm, not the exception.

For example, from a technological perspective, take the last 250 years and the advent of the steam engine and the Industrial Revolution itself. We saw productivity enhanced as well as the upending of the global economic way of doing business. Centuries-old industries were extinguished in a matter of years, social dynamics evolved rapidly with wealth and income inequality growing at a rapid pace alongside the redrawing of political and financial institutions to cope with the rapid urbanisation and mechanisation of society.

From a geopolitical perspective, the Napoleonic Wars and the subsequent Congress of Vienna reshaped trade and political maps for over a century in Europe. The Great Depression and the two World Wars on either side of it altered trading relationships and fragmented previously-strong geopolitical relationships which ultimately led to the creation of global institutions such as the UN, IMF and World Bank to restore stability and trust. And of course, perhaps most of all, the creation of what is now the European Union, a peace project like no other and which has brought economic benefits to millions of people across the continent.

These relatively modern historical precedents – I am resisting the temptation to go back further in history – act as a reminder that today's challenges – from economic crashes, geopolitical tensions and the fragmentation of economic relationships – are simply new iterations of an enduring message. As someone once said, "there is nothing more certain and unchanging than uncertainty and change".

As we face into a period of further uncertainty, both from geopolitical transitions and the more familiar transitions of an ageing society, a changing climate and rapid technological innovation, the importance of economic resilience stands out. Economies must be resilient and robust enough to withstand the 'Knightian uncertainty' – when it is difficult to assign probabilities to imaginable outcomes – that frequently impact on our lived reality. Instead of allowing ourselves "fall into the role of a victim" of circumstance, we can and should take matters into our own hands.

Current inflationary outlook

But back to my first proposition. Successful economies need stable and predictable prices.

A year ago, inflationary pressures had eased somewhat, and it was becoming clearer that there would be a gradual convergence of inflation to our 2 per cent target during 2025. The latest projections – from September – and the incoming data that I have seen so far lead me to feel confident that inflation will be at target over the medium term, in line with our price stability objective (although, again, there will be a new set of projections next week incorporating the latest data and information).

To learn more:
https://www.centralbank.ie/news/article/speech-economic-resilience-what-next-governor-gabriel-makhlouf-10-december-2025

Number 3

EIOPA flags financial stability risks related to private credit, a weakening dollar and global interconnectedness

The European Insurance and Occupational Pensions Authority (EIOPA) published its December 2025 Financial Stability Report in which it analyses the risks and vulnerabilities facing European insurers and occupational pension funds in a period marked by economic fragility, subdued growth and high uncertainties about the future of international collaboration and its implications on the economy.

The report also features five deep dives into current and relevant developments, covering insurers' and occupational pension funds' exposures to private credit, risks stemming from a weakening dollar, global market interconnectedness, cyber risk as a potential systemic threat, and the role of AI in amplifying existing systemic vulnerabilities.

The macroeconomic context throughout 2025 has been influenced by the prospect of a retreat from international cooperation, ongoing uncertainties around trade and geopolitical tensions as well as concerns over elevated debt levels.

Inflation is hovering around the 2% target and monetary policy has stabilized, yet high borrowing costs continue to put pressure on public finances. While financial markets have remained resilient, valuations appear optimistic about the impact of tariffs on the economy and about the extent to which the AI boom will boost productivity.

Despite the fragile economic environment, insurers and occupational pension funds have stayed resilient and well-capitalised. Median Solvency Capital Requirements (SCR) for life insurers stand at 235%, at 214% for non-life insurers and at 218% for composite insurers. IORPs' aggregate funding ratio has improved and is now above 120%. However, adverse developments in the current environment could trigger a repricing of risk premia, underscoring the need for continued monitoring and prudent risk management.

Beyond these developments, EIOPA's Financial Stability Report also analyses five focus areas with relevance to insurers, occupational pension funds and supervisors:

1. Private credit investments: This topical focus examines European insurers' and IORPs' exposure to private credit and the vulnerabilities associated with such investments. Private credit markets have grown substantially in recent years. While early allocations were driven by a search for yield in a low-interest-rate environment, investment has continued to expand even after risk-free rates began to rise. Private assets typically offer an illiquidity premium and portfolio

diversification benefits, making them particularly attractive to long-term investors such as life insurers and pension funds.

According to EIOPA's analysis, insurers' private credit exposure totalled €514 billion (or 5.1% of total assets) at the end of 2024, while exposure for IORPs stood at €128 billion (or 4.4% of total assets). Mortgages and loans accounted for around two-thirds of private credit exposures, followed by unlisted or untraded corporate bonds and collateralised securities subject to credit risk.

Exposures show considerable cross-country variation, alongside sectoral and geographical concentrations that can offset diversification gains and amplify losses in a downturn. Private credit is also characterised by higher credit and liquidity risk, valuation uncertainty and hidden leverage, which, if not properly managed, can significantly affect exposed undertakings. Continued monitoring of private credit exposures – including concentration metrics – remains essential to mitigating the build-up of potential systemic risks.

2. Dollar depreciation: The second focus tracks the notable decline in the value of the US dollar throughout 2025 and examines European insurers' and occupational pension funds' exposure to dollar-denominated assets, along with the related risks and mitigating factors. EIOPA's analysis indicates that European insurers and IORPs collectively held around €1.8 trillion in US dollar assets at the end of last year.

While the exposures are sizeable, it is important to note that insurers and occupational pension funds share market risk with policyholders and beneficiaries in the case of unit-linked and defined contribution portfolios. To manage currency risk on their investments, IORPs typically use derivatives to hedge FX risk, while also benefitting from implicit hedging when the US dollar and US equity markets move in opposite directions.

On the other hand, insurers face a more complex set of challenges, as a weakening dollar can affect not only their investments but also their liabilities and profitability. To mitigate these risks, insurers rely on hedging strategies, currency-specific asset-liability matching, reinsurance, and risk-sharing with policyholders. Overall, the findings underline the importance of continued monitoring of hedging practices and FX risk management.

3. Interconnectedness with global markets: The third article provides an overview of the exposure of European insurers to non-EEA countries in terms of assets, liabilities and underwriting to gauge the significance of these exposures from a financial stability perspective. While international exposures can offer diversification benefits and improved returns, they can also increase market, currency and counterparty risks as well as underwriting vulnerabilities.

The data shows that EEA insurers allocate approximately 13% (€1.24 trillion) of their direct investments to non-EEA issued instruments. Almost half of these exposures (46%) are linked to the United States, followed by the United Kingdom, which receives 22% of direct non-EEA investments.

Looking at ceded business, nearly 28% of the risks are transferred outside the EEA, with the UK taking 42.1% of these transfers, followed by Bermuda (26.5%) and Switzerland (22.1%) – all major markets in the global reinsurance industry. These linkages warrant close monitoring given rising geoeconomic tensions and structural shifts in the life insurance business like asset-intensive reinsurance and the transfer of risks to a limited number of jurisdictions.

4. Cyber risks: The fourth topical focus explores how cyber risks, once viewed primarily as IT issues, have evolved into a macrofinancial stability concern. In today's highly interconnected digital economy, cyber risk has become a persistent structural threat.

Technological interdependencies that cut across sectors and borders create vulnerabilities to both malicious and accidental incidents, with the potential to generate large economic and insured losses—even from a single event. These vulnerabilities underscore the need for closer cooperation, improved data collection and more advanced modelling of accumulation risks.

5. AI's impact on the insurance industry: This fifth and final article examines the growing use of artificial intelligence in the insurance sector and its potential implications for financial stability. While most current applications remain operational, future use cases in underwriting, investment and risk management could amplify existing systemic vulnerabilities.

Key channels include correlated behaviour driven by the use of similar models, herding in investment strategies, greater third-party dependencies, demutualisation pressures arising from increasingly granular risk segmentation, and risks linked to the development of insurance markets covering AI-related failures themselves.

To learn more:
https://www.eiopa.europa.eu/eiopa-flags-financial-stability-risks-related-private-credit-weakening-dollar-and-global-2025-12-15_en

Number 4

The EBA provides guidance to banks on enhanced reporting requirements for operational risk ahead of new June 2026 reference date

The European Banking Authority (EBA) published clear guidance for banks on how to manage enhanced reporting requirements for operational risk, following the postponement of the first reference date under the amended Implementing Technical Standards (ITS).

This move comes after the European Commission adopted Regulation (EU) 2025/2475, which delays the application of new operational risk reporting obligations to the end of June 2026.

Key points for institutions:

- Extended preparation period: Banks now have until the end of June 2026, rather than March 2026, to comply with the new reporting requirements, ensuring at least six months to adapt to the change after the Regulation enters into force.

- Guidance on reporting: the EBA clarifies that institutions should use the COREP OF module (release 4.2) for operational risk reporting. Templates C 16.02, C 16.03, and C 16.04 will not be required for the March 2026 reference date, and their first mandatory submission will be in June 2026. However, banks may choose to report these templates voluntarily from March 2026.

- Ongoing requirements: Institutions must still report template C 16.01 using the updated technical tables in release 4.2, but information on "other operating expenses" will not be required for March 2026.

- Updated instructions and other IT solutions: the EBA has published amended instructions for both reporting and disclosure of operational risk, correcting references and ensuring consistency. They shall apply starting with reference date end June 2026. These updates are available on the EBA website, along with translations in all EU languages. The "Overview of the IT solutions" file, which covers the reporting obligations by linking the Articles of the ITS with the ITS templates to be reported, has also been revised to help banks navigate the amended requirements.

- Support for implementation: the EBA will soon update its signposting tool to reflect the new obligations. The mapping tool, which links reporting and disclosure templates, has also been updated.

Next steps

Banks are encouraged to consult the latest instructions and tools on the EBA website to ensure a smooth transition to the new reporting framework. The EBA remains committed to supporting institutions with clear, timely guidance as they prepare for the enhanced operational risk reporting regime.

To learn more:
https://www.eba.europa.eu/publications-and-media/press-releases/eba-provides-guidance-banks-enhanced-reporting-requirements-operational-risk-ahead-new-june-2026

Number 5

Adverse scenarios for the 2025 European Insurance and Occupational Pensions Authority's EU-wide pension fund stress test exercise

ESRB
European Systemic Risk Board
European System of Financial Supervision

In accordance with its mandate, the European Insurance and Occupational Pensions Authority (EIOPA), in cooperation with the European Systemic Risk Board (ESRB), initiates and coordinates EU-wide stress tests to assess the resilience of institutions for occupational retirement provision (hereafter "pension funds") to adverse developments.

For this purpose, the ESRB, in collaboration with the European Central Bank (ECB) and EIOPA, provides the calibration of the adverse market stress parameters. This document presents the adverse scenarios that pension funds are required to use in the 2025 EU-wide stress test.

This year's pension fund stress test focuses on liquidity risk, with a view to assessing liquidity strains stemming from an episode of instantaneous market turmoil with shocks to asset prices and potential margin calls.

EIOPA asked the ESRB to provide two adverse macro-financial scenarios for this stress test: a "yield curve up" scenario and a "yield curve down" scenario.

The stress test is a scenario-based analysis that measures how pension funds would fare given hypothetical adverse economic developments.

The adverse scenarios describe shocks to key financial variables triggered by the materialisation of risks to which pension funds in the EU are exposed.

Accordingly, the scenarios reflect a hypothetical situation and should not be considered as forecasts of the most likely negative shocks to the financial system.

The scenario horizon is five days. The shock profiles of the adverse scenarios are one-off, instantaneous shifts in asset prices relative to their end-2024 levels without further changes over the five-day horizon.

In the adverse scenarios, no monetary or fiscal policy actions are assumed beyond what is implicitly captured in the historical asset price movements on which the scenarios were calibrated.

The adverse scenarios were approved by the ESRB General Board on 18 March 2025 and sent to EIOPA on 27 March 2025.

Systemic risks and vulnerabilities addressed by the scenarios

The scenarios reflect the ESRB's assessment of prevailing sources of systemic risks identified for the EU financial system as of March 2025.

These include:

(i) the materialisation of geopolitical and/or macro-financial risks resulting in balance sheet stress for the private sector, notably for non-financial corporations;

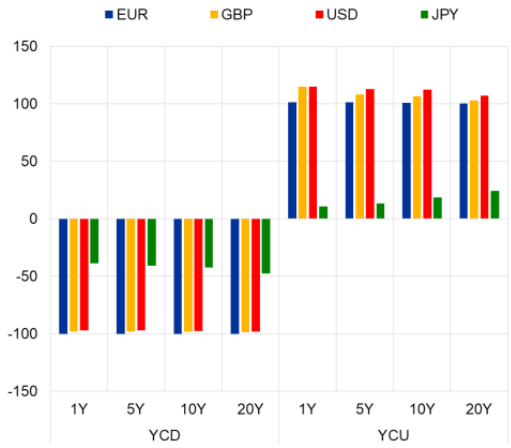
(ii) the materialisation of geopolitical and/or macro-financial risks triggering a disorderly market correction, possibly amplified by the non-banking financial sector;

(iii) unfavourable growth and debt financing cost dynamics triggered by increased borrowing needs, leading to a re-emergence of sovereign debt sustainability concerns;

(iv) deteriorating asset quality and funding liquidity risk for the banking sector triggered by adverse macro-financial or geopolitical shocks;

(v) the materialisation of vulnerabilities in the real estate sector, particularly in the commercial real estate sector.

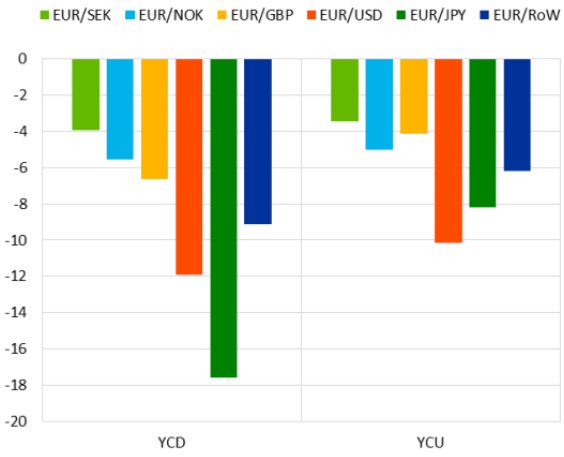
Chart 1
Shocks to swap rates under the YCD and YCU scenarios
(absolute change in basis points)



Sources: ECB and ECB/ESRB calculations.

Notes: YCD and YCU stand for the "yield curve down" and the "yield curve up" scenarios respectively. The same holds for Charts 2-6.

Chart 2
Shocks to euro foreign exchange rates under the YCD and YCU scenarios
(relative changes in percentages)



Sources: ECB and ECB/ESRB calculations.

The adverse scenarios are calibrated also to replicate certain key features of relevant episodes like the September 2022 gilt crisis that caused liquidity stress in UK pension funds. Both scenarios feature strong shifts in swap rate curves as well as a depreciation of the domestic currency.

While events with a rapid unravelling of imbalances like the one seen during the UK gilt crisis have not been observed in the euro area, these are still considered unlikely but plausible in the current context.

Both scenarios are calibrated to be severe, consistent with a materialisation of tail risks amid high geopolitical uncertainty stemming from trade disputes and multiple conflicts around the world. In the “yield curve up” scenario, the escalation of geopolitical tensions affects the supply side of the economy, resulting in inflationary effects and triggering an upward shift in swap rate curves.

Conversely, in the “yield curve down” scenario, geopolitical tensions affect the demand side more, triggering a persistent recessionary and disinflationary environment and, as a result, a downward shift in swap rate curves.

To learn more:
https://www.eiopa.europa.eu/document/download/12f0d16c-ce16-45b5-8a03-13baacac398a_en?filename=2025%20IORP%20stress%20test%20-%20Adverse%20scenarios%20for%20EU-wide%20pension%20fund%20stress%20test%20exercise.pdf

Number 6

CISA Unveils Enhanced Cross-Sector Cybersecurity Performance Goals

New Benchmarks Empower Organizations to Counter Emerging Threats, Build Cyber Resilience, and Strengthen Governance

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

The Cybersecurity and Infrastructure Security Agency (CISA) released version 2.0 of its Cross-Sector Cybersecurity Performance Goals (CPGs), offering organizations a more robust framework for integrating cybersecurity into daily operations.

You may visit:
https://www.cisa.gov/cybersecurity-performance-goals-2-0-cpg-2-0

The updated CPGs align with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0, incorporates three years of operational insights, and address emerging threats through data-driven, actionable guidance. These enhancements are designed to promote accountability, improve risk management, and support strategic cybersecurity governance across sectors.

The Cross-Sector CPGs represent a targeted subset of best practices, carefully selected through extensive consultation with industry leaders, government stakeholders, and cybersecurity experts. Designed to meaningfully reduce risks to critical infrastructure and safeguard the American public, these goals offer a practical starting point for small and medium-sized organizations. By focusing on a limited set of high-impact actions, the CPGs help prioritize cybersecurity investments that deliver measurable improvements in resilience and risk reduction.

The updated goals offer expanded and clarified guidance across key cybersecurity domains—including account and device security, data protection, governance, vulnerability management, supply chain risk, and incident response and recovery. Building on the foundation of version 1.0.1, CPG 2.0 introduces several notable improvements:

- Governance Emphasis: A new "Govern" function underscores the critical role of organizational leadership in cybersecurity, regrouping existing goals and introducing two new ones focused on risk management strategy, policy development, and executive accountability.

- Unified Goal Structure: Operational Technology (OT) and Information Technology (IT) goals are now consolidated into universal goals, eliminating silos across IT, Internet of Things (IoT), and OT environments.

- Threat-Responsive Expansion: New goals address emerging threats, third-party risk, zero trust architecture, and incident communication protocols.

- Streamlined Framework: Redundant, unclear, or underutilized goals have been removed to improve clarity and usability.

- Enhanced Documentation: Each goal now includes clearer methodology and supporting materials to reduce guesswork and improve implementation.

Cybersecurity Performance Goals 2.0 (CPG 2.0)

The CPGs 2.0 are voluntary practices with high-impact security actions that outline the highest-priority baseline that measures businesses and critical infrastructure owners of all sizes can take to protect themselves against cyber threats. They were developed based on CISA's operational data, research on the current threat landscape, and collaboration with government, industry groups, and private sector experts to receive input and feedback.

"Over the past year, CISA has engaged extensively with hundreds of stakeholders across both the public and private sectors to ensure the updated goals reflect real-world challenges and operational realities," said Madhu Gottumukkala, Acting CISA Director. "Version 2.0 demonstrates our commitment to listening to and incorporating partner feedback to deliver practical, outcome-driven guidance that organizations can act on. These goals are applicable across all critical infrastructure sectors and offer foundational protection for organizations regardless of their cybersecurity maturity. We encourage all organizations to adopt the new CPGs and continue sharing feedback to help us refine future iterations."

The Cross-Sector CPGs serve three primary purposes:

- Provide measurable actions that critical infrastructure entities can take to achieve a basic level of cybersecurity.

- Bridge communication gaps between IT/OT technical staff and organizational leadership to align on cybersecurity priorities.

- Support strategic planning by offering clear guidance that informs both near- and long-term cybersecurity investments.

CISA encourages organizations to adopt the voluntary Cross-Sector CPGs. To learn more about the updated Cybersecurity Performance Goals and how they can support your organization's cybersecurity program, visit Cross-Sector Cybersecurity Performance Goals and Objectives.

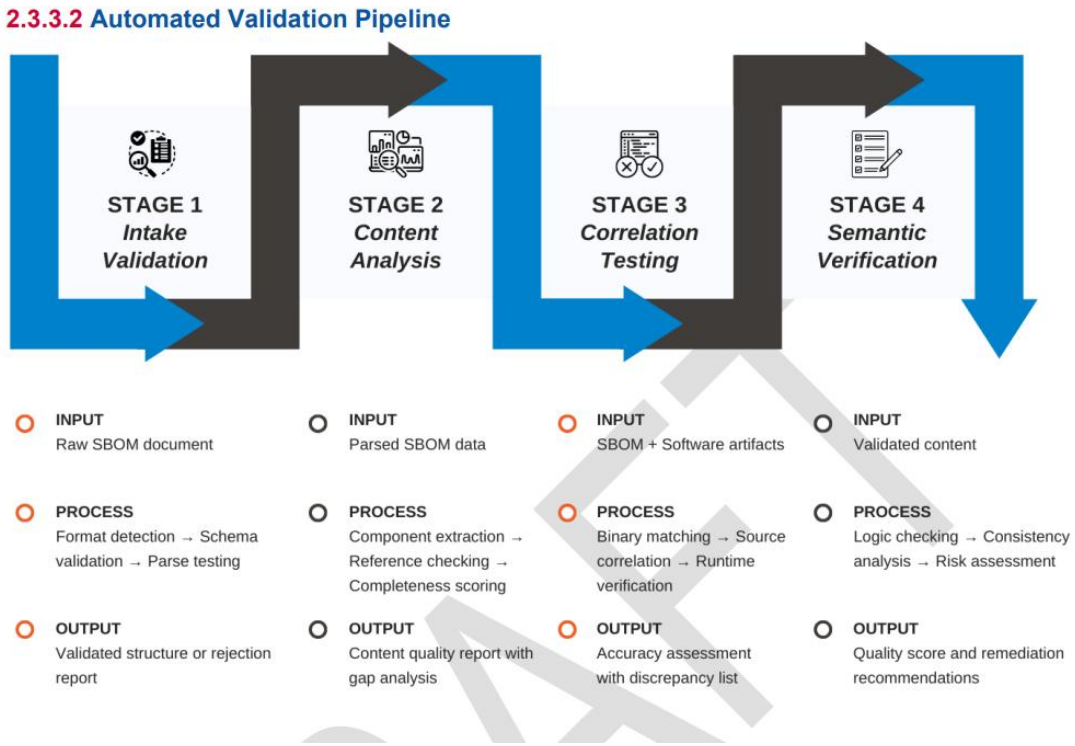
To learn more:
https://www.cisa.gov/news-events/news/cisa-unveils-enhanced-cross-sector-cybersecurity-performance-goals

Number 7

Call for Feedback: Advancing Software Supply Chain Security together!

ENISA invites industry stakeholders and interested parties to provide their feedback on the draft SBOM Landscape Analysis and the Technical Advisory for Secure Use of Package Managers.

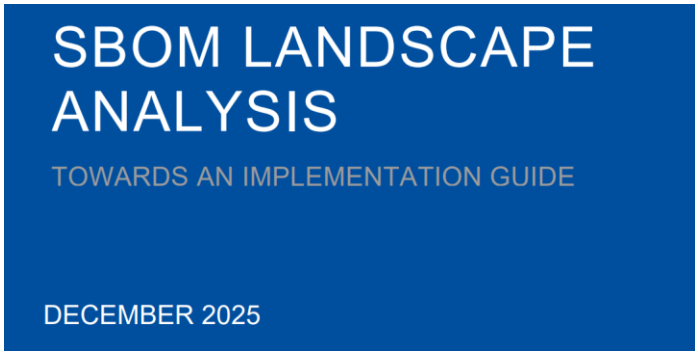
ENISA works to strengthen cybersecurity by promoting cybersecurity-by-design and cybersecurity-by-default in the EU market. The EU is prioritising the security of all digital products and the protection of end-users, safeguarding our shared connected ecosystem. Through the launch of the two new public consultations, the Agency aims to engage with professionals working in product security and development to provide meaningful guidance and support in advancing cybersecurity across the ecosystem.



SBOM Landscape Analysis: Towards an Implementation Guide

Software Bills of Materials (SBOM) implementation is a significant step for organisations to enhance management, transparency and resilience of their systems. ENISA has compiled a draft report of comprehensive yet practical

guidance for implementing Software Bill of Materials practices within organisations of varying sizes and capabilities.



You may provide your feedback by 23 January 2025 at 23:59 CET by taking part in the survey:
https://ec.europa.eu/eusurvey/runner/SBOM_Analysis_Implementation_Guide

To learn more:
https://www.enisa.europa.eu/news/call-for-feedback-advancing-software-supply-chain-security-together

Number 8

Amazon Threat Intelligence identifies Russian cyber threat group targeting Western critical infrastructure

As we conclude 2025, Amazon Threat Intelligence is sharing insights about a years-long Russian state-sponsored campaign that represents a significant evolution in critical infrastructure targeting: a tactical pivot where what appear to be misconfigured customer network edge devices became the primary initial access vector, while vulnerability exploitation activity declined.

This tactical adaptation enables the same operational outcomes, credential harvesting, and lateral movement into victim organizations' online services and infrastructure, while reducing the actor's exposure and resource expenditure.

Going into 2026, organizations must prioritize securing their network edge devices and monitoring for credential replay attacks to defend against this persistent threat.

Based on infrastructure overlaps with known Sandworm (also known as APT44 and Seashell Blizzard) operations observed in Amazon's telemetry and consistent targeting patterns, we assess with high confidence this activity cluster is associated with Russia's Main Intelligence Directorate (GRU). The campaign demonstrates sustained focus on Western critical infrastructure, particularly the energy sector, with operations spanning 2021 through the present day.

Technical details

Campaign scope and targeting: Amazon Threat Intelligence observed sustained targeting of global infrastructure between 2021-2025, with particular focus on the energy sector. The campaign demonstrates a clear evolution in tactics.

Timeline:

- 2021-2022: WatchGuard exploitation (CVE-2022-26318) detected by Amazon MadPot; misconfigured device targeting observed
- 2022-2023: Confluence vulnerability exploitation (CVE-2021-26084, CVE-2023-22518); continued misconfigured device targeting
- 2024: Veeam exploitation (CVE-2023-27532); continued misconfigured device targeting
- 2025: Sustained targeting of misconfigured customer network edge device targeting; decline in N-day/zero-day exploitation activity

Primary targets:

- Energy sector organizations across Western nations
- Critical infrastructure providers in North America and Europe
- Organizations with cloud-hosted network infrastructure

Commonly targeted resources:

- Enterprise routers and routing infrastructure
- VPN concentrators and remote access gateways
- Network management appliances
- Collaboration and wiki platforms
- Cloud-based project management systems

Targeting the "low-hanging fruit" of likely misconfigured customer devices with exposed management interfaces achieves the same strategic objectives, which is persistent access to critical infrastructure networks and credential harvesting for accessing victim organizations' online services.

The threat actor's shift in operational tempo represents a concerning evolution: while customer misconfiguration targeting has been ongoing since at least 2022, the actor maintained sustained focus on this activity in 2025 while reducing investment in zero-day and N-day exploitation.

The actor accomplishes this while significantly reducing the risk of exposing their operations through more detectable vulnerability exploitation activity.

Credential harvesting operations

While we did not directly observe the victim organization credential extraction mechanism, multiple indicators point to packet capture and traffic analysis as the primary collection method:

- Temporal analysis: Time gap between device compromise and authentication attempts against victim services suggests passive collection rather than active credential theft
- Credential type: Use of victim organization credentials (not device credentials) for accessing online services indicates interception of user authentication traffic
- Known tradecraft: Sandworm operations consistently involve network traffic interception capabilities

- Strategic positioning: Targeting of customer network edge devices specifically positions the actor to intercept credentials in transit

Infrastructure targeting

Compromise of infrastructure hosted on AWS: Amazon's telemetry reveals coordinated operations against customer network edge devices hosted on AWS. This was not due to a weakness in AWS; these appear to be customer misconfigured devices.

Network connection analysis shows actor-controlled IP addresses establishing persistent connections to compromised EC2 instances operating customers' network appliance software. Analysis revealed persistent connections consistent with interactive access and data retrieval across multiple affected instances.

Credential replay operations: Beyond direct victim infrastructure compromise, we observed systematic credential replay attacks against victim organizations' online services. In observed instances, the actor compromised customer network edge devices hosted on AWS, then subsequently attempted authentication using credentials associated with the victim organization's domain against their online services. While these specific attempts were unsuccessful, the pattern of device compromise followed by authentication attempts using victim credentials supports our assessment that the actor harvests credentials from compromised customer network infrastructure for replay against target organizations' online services. Actor infrastructure accessed victims' authentication endpoints for multiple organizations across critical sectors through 2025, including:

- Energy sector: Electric utility organizations, energy providers, and managed security service providers specializing in energy sector clients
- Technology/cloud services: Collaboration platforms, source code repositories
- Telecommunications: Telecom providers across multiple regions

Geographic distribution: The targeting demonstrates global reach:

- North America
- Europe (Western and Eastern)
- Middle East
- The targeting demonstrates sustained focus on the energy sector supply chain, including both direct operators and third-party service providers with access to critical infrastructure networks.

Campaign flow:

1. Compromise customer network edge device hosted on AWS.

2. Leverage native packet capture capability.

3. Harvest credentials from intercepted traffic.

4. Replay credentials against victim organizations' online services and infrastructure.

5. Establish persistent access for lateral movement.

Infrastructure overlap with "Curly COMrades"

Amazon Threat Intelligence identified threat actor infrastructure overlap with group Bitdefender tracks as "Curly COMrades." We assess these may represent complementary operations within a broader GRU campaign:

- Bitdefender's reporting: Post-compromise host-based tradecraft (Hyper-V abuse for EDR evasion, custom implants CurlyShell/CurlCat)

- Amazon's telemetry: Initial access vectors and cloud pivot methodology

This potential operational division, where one cluster focuses on network access and initial compromise while another handles host-based persistence and evasion, aligns with GRU operational patterns of specialized subclusters supporting broader campaign objectives.

Amazon's response and disruption

Amazon remains committed to helping protect customers and the broader internet ecosystem by actively investigating and disrupting sophisticated threat actors.

Immediate response actions:

- Identified and notified affected customers of compromised network appliance resources

- Enabled immediate remediation of compromised EC2 instances

- Shared intelligence with industry partners and affected vendors

- Reported observations to network appliance vendors to help support security investigations

Disruption impact: Through coordinated efforts, since our discovery of this activity, we have disrupted active threat actor operations and reduced the attack surface available to this threat activity subcluster.

We will continue working with the security community to share intelligence and collectively defend against state-sponsored threats targeting critical infrastructure.

Defending your organization

Immediate priority actions for 2026

Organizations should proactively monitor for evidence of this activity pattern:

1. Network edge device audit

Audit all network edge devices for unexpected packet capture files or utilities.
Review device configurations for exposed management interfaces.
Implement network segmentation to isolate management interfaces.
Enforce strong authentication (eliminate default credentials, implement MFA).

2. Credential replay detection

Review authentication logs for credential reuse between network device management interfaces and online services.
Monitor for authentication attempts from unexpected geographic locations.
Implement anomaly detection for authentication patterns across your organization's online services.
Review extended time windows following any suspected device compromise for delayed credential replay attempts.

3. Access monitoring

Monitor for interactive sessions to router/appliance administration portals from unexpected source IPs.
Examine whether network device management interfaces are inadvertently exposed to the internet.
Audit for plain text protocol usage (Telnet, HTTP, unencrypted SNMP) that could expose credentials.

4. IOC review

Energy sector organizations and critical infrastructure operators should prioritize reviewing access logs for authentication attempts from the IOCs listed below.

To learn more:
https://aws.amazon.com/blogs/security/amazon-threat-intelligence-identifies-russian-cyber-threat-group-targeting-western-critical-infrastructure/

Number 9

The cyber threat to Canada's water systems: Assessment and mitigation

Government of Canada

Audience

This report is part of a series of cyber threat assessments focused on Canada's critical infrastructure. It is intended for leaders of organizations in the water sector, cyber security professionals with a water or wastewater asset to protect, and the general reader with an interest in the cyber security of critical infrastructure. For guidance on technical mitigation of these threats, see the Mitigation section or contact the Canadian Centre for Cyber Security (the Cyber Centre).

This assessment is Unclassified/TLP:CLEAR. TLP:CLEAR is used when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

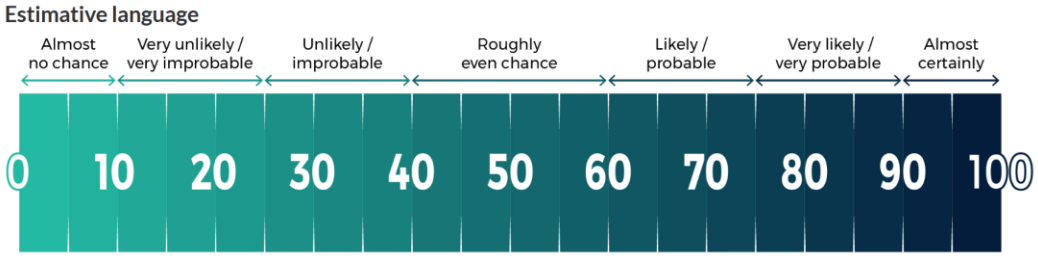
Assessment base and methodology

The key judgements in this assessment rely on reporting from multiple sources, both classified and unclassified. The judgements are based on the knowledge and expertise in cyber security of the Cyber Centre.

Defending the Government of Canada's information systems provides the Cyber Centre with a unique perspective to observe trends in the cyber threat environment, which also informs our assessments.

The Communications Security Establishment Canada's foreign intelligence mandate provides us with valuable insight into adversary behaviour in cyberspace. While we must always protect classified sources and methods, we provide the reader with as much justification as possible for our judgements.

Our judgements are based on an analytical process that includes evaluating the quality of available information, exploring alternative explanations, mitigating biases and using probabilistic language. We use terms such as "we assess" or "we judge" to convey an analytic assessment. We use qualifiers such as "possibly", "likely" and "very likely" to convey probability.



The assessments and analysis are based on information available as of May 31, 2025.

Message from the Head of the Cyber Centre

I spend a lot of time looking at threats most people never see. They are quiet, often hidden, yet capable of real-world consequences. Among the most critical are the cyber threats facing Canada's water and wastewater systems. These systems are the backbone of modern life, yet they're often out of sight and out of mind. When they function, no one notices. When they fail, everyone does.

This assessment is meant to bring clarity to a topic that can feel abstract or overly technical. Cyber threats to water infrastructure are growing, evolving quickly, and can affect every community in Canada. You don't need to be an engineer or a cyber security expert to understand why this matters. Clean water is essential, and the systems that deliver it are now largely digital – meaning they are vulnerable to the same kinds of cyber threats that target businesses and governments around the world.

We've seen an unmistakable shift in recent years. Cybercriminals are more sophisticated, state-sponsored actors are more willing to target essential services, and disruptive tools are easier to access. Water systems now face a threat landscape they were never designed to withstand.

Whether you're a critical infrastructure executive, an elected official, or a policymaker, I want to emphasize that cyber security for water systems is not just a technical issue, it is a public safety issue, an economic stability issue, and ultimately a public trust issue. Leadership matters. The choices you make about investment, governance, and preparedness will determine our collective resilience in the years ahead.

But this is not a message of alarm; it is a message of readiness. Across Canada, utilities, municipalities, and provincial and territorial partners have shown a strong commitment to improving their cyber resilience. What's needed now is a clear-eyed analysis of the cyber threats facing our water systems in Canada. That's what this assessment provides.

My hope is that it empowers decision-makers to act confidently, ask the right questions, and support the people who keep these systems running. Cyber threats aren't going away, but with awareness and a steady commitment to resilience, we can stay ahead of them.

Sincerely,
Rajiv Gupta, Head of the Canadian Centre for Cyber Security

Key judgements

- We assess that operational technology (OT) networks that monitor and control physical processes are very likely the primary target for actors seeking to disrupt water systems.

- We assess that financially motivated cybercriminals are the most likely cyber threat to affect water systems. We assess that cybercriminals will almost certainly continue to exploit water sector organizations and systems through extortion tied to ransomware, exploiting stolen information, and business email compromise (BEC). We assess that ransomware is almost certainly the most significant cyber threat to the reliable supply of water in Canada due to the potential impacts against OT systems.

- We assess that water systems are almost certainly a strategic target for state-sponsored actors to project power through disruptive or destructive cyber threat activity. We assess that state-sponsored actors have almost certainly developed pre-positioned access to Canadian water systems. However, we judge that these actors would likely only disrupt those water systems in times of crisis or conflict between states.

- Non-state cyber actors are a growing threat to Canada's critical infrastructure (CI). We assess that non-state actors will very likely continue to opportunistically compromise and disrupt Internet-exposed water system OT within Canada, especially in connection to major geopolitical events.

Canada's water sector

Good public and environmental health depend on access to clean water. Drinking water, stormwater and wastewater treatment systems (collectively: water systems) have many important economic, environmental, and safety uses. A loss of water does not just affect residents but also can have effects on other critical infrastructure.

Figure 1: Critical infrastructure

Critical infrastructure refers to the processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government.

For example, in 2024, water main breaks in Calgary and Montreal resulted in cascading impacts on other systems, including hospitals, fire prevention and universities. For these reasons and others, our water systems are considered part of Canada's critical infrastructure (Figure 1). Any disruption in the water system is not only a threat to public health and safety, but also a threat to public confidence, the environment and the economy. As a result, the cyber security of our water systems is vital to Canada's national security.

The threat surface of Canada's water systems

A water system generally includes the services and infrastructure to safely and reliably obtain, store, filter and distribute potable water, divert runoff and floodwater as well as remove, collect and treat wastewater. Canada has thousands of water systems that vary greatly in size.

A small number of large water utilities serve major urban areas while international organizations manage shared systems. Meanwhile, many small systems are owned and operated by municipalities, other levels of government, Indigenous communities, private sector companies and individual citizens.

Water systems operate in a variety of ways. Many are completely manual or even passive systems that require little to no active management, including most small water supplies and stormwater systems.

Large urban water systems, in contrast, are usually geographically dispersed, industrial systems operated from a digital control environment. These include many remotely managed OT devices integrated into dams, pumping stations, and treatment facilities. These systems also extend into a web of connected suppliers of digital products and services.

Many of these water systems are managed out of municipal or community offices and are exposed to all the cyber threats encountered by public-facing organizations. The more internet-connected assets an organization has, the larger the threat surface. A larger threat surface implies an increase in the cyber threat the organization faces.

In addition to increasing internet connectivity, most water systems are operated by small public sector organizations and frequently face challenges that can negatively influence cyber security, including low financial resources, aging physical and digital infrastructure and a shortage of cyber security expertise.

The role of operational technology in our water systems

Operators use industrial OT including supervisory control and data acquisition (SCADA) and industrial Internet of things (IIoT) devices to manage large water systems and address issues like population growth, outdated infrastructure and declining revenue.

These systems are used to control water system equipment like dam gates, valves and pumps and to monitor sensors such as chemical detectors and flowrate monitors. The OT in water systems is continually evolving and is increasingly managed through digital devices with embedded computing and communications abilities.

This process, called digital transformation or digitalization, has allowed OT asset operators like those in the water sector to connect their OT devices to operating centres, corporate networks and, increasingly, directly to the internet.

A 2021 survey counted over 60,000 OT-related network interfaces in Canada. In 2023, a similar survey conducted on internet-connected devices associated mainly with water systems in the U.S. and UK found a relatively low level of basic cyber hygiene. Almost half of the devices could be manipulated without any authentication required.

Unfortunately, the management efficiency and savings gained from connecting digitally transformed OT also exposes the water system to cyber threats.

For example, in early 2000, an employee was fired from a company providing services to Maroochy Water Services in Queensland, Australia. The individual retained remote access to the network of OT devices in the pumping stations of the wastewater treatment system.

He used this access to issue malicious commands to the OT devices that ultimately caused nearly a million litres of raw sewage to be discharged into local parks and rivers, causing severe environmental harm, according to officials.

This was the first example of a remote access in a public water system being used to disrupt or sabotage OT systems and illustrates the potential for cyber threats to jeopardize public and environmental safety and the local economy.

We assess that operational technology (OT) networks that monitor and control physical processes are very likely the primary target for actors seeking to disrupt water systems.

On the rise: Cyber threats to supply chains

Water system utilities often depend on a diverse supply chain of digital products and services to operate, maintain and modernize their OT assets. The supply chain for these products and services includes manufacturers, vendors, integrators, contractors and service providers. Water system OT's dependency on the supply chain is a critical vulnerability that gives cyber actors inside information on and opportunities for access to otherwise protected OT systems.

Cyber threat actors target organizations' digital supply chains to collect business and contextual information for use in social engineering attacks or to collect organizational network and system information to support future cyber attacks.

Activity against the digital supply chain can also be an indirect route to gain access to the target organization's networks in situations where there is continuous information transfer, for example software updates, or remote network access connections between the organization and its suppliers. In late 2019, a sophisticated cyber threat actor compromised the software-as-a-service provider, SolarWinds.

The actors, attributed to Russia's intelligence services, used their access to SolarWinds' development environment to embed malicious code into a software update. The compromised update provided the actors access to thousands of client networks worldwide, including over 100 in Canada.

Publicly available cyber tools are increasing the volume and effectiveness of cyber threat activity

We assess it almost certain that cyber threat actors are increasingly using publicly available cyber tools to gain and maintain access to CI networks, making it easier for threat actors of all levels of sophistication to target water sector OT.

The wide availability of these tools, including legitimate penetration testing tools like Cobalt Strike, has lowered the barrier to entry to cyber threat activity and increased the capacity for cyber threat actors to gain, maintain, and expand access to target systems.

The state-sponsored cyber threat to water systems

We assess that water systems are almost certainly a strategic target for state-sponsored actors to project power through disruptive or destructive cyber threat activity. State-sponsored actors pre-position for this activity by identifying and gaining access to Internet-connected OT systems or IT networks from which they can laterally move to OT systems. Once in the target network, they collect information on assets within the network to identify opportunities for disruptive or destructive action. For example, this could mean causing water tanks to overflow or changing the chemical balance of water treatment processes. We assess that state-sponsored cyber threat actors have almost certainly developed pre-positioned access to Canadian water systems. However, we judge that these actors would likely only disrupt those water systems in times of crisis or conflict between states.

To learn more:
https://www.cyber.gc.ca/en/guidance/cyber-threat-canadas-water-systems-assessment-mitigation

Number 10

The Cyber Defense Review - Resilient Dependencies: Preparing to Fight Through Cyber Disruption

Lt. Gen. Maria B. Barrett, U.S. Army Cyber Command, Fort Gordon, GA, USA

THE CYBER DEFENSE REVIEW

In a volatile threat environment, the Army's readiness and ability to execute missions at home and abroad increasingly hinge on digital dependencies spanning commercial software, IT/OT infrastructure, utilities, and the organic industrial base.

This opener frames a cohesive approach to mission thread resilience across the Unified Network, emphasizing three imperatives: partner early and often with program managers, vendors, contractors, and local utilities to rehearse crisis response and establish shared understanding; procure secure by design capabilities with transparent vulnerability disclosure and rapid patching; and make data informed, commander owned risk decisions that enable formations to "fight through" disruption.

Drawing lessons from the Army Cyber Institute's Jack Voltaic workshops and the inaugural Army Defensive Cyberspace Operations Optimization Conference, the article illustrates how civil military interdependencies can cascade and how rehearsals reveal hidden assumptions.

A "fort to port" vignette, where a cyber compromise of national rail switching triggers operational delays, shows the value of synchronized public-private response, near real-time operational data, and flexible branches and sequels.

The piece calls for acquisition leaders to weigh vendor track records on zero days and patch latency, signals the need to report and coordinate through ARCYBER's Information Warfare Operations Center and NETCOM's Global Cyber Center, and argues for a whole-of-nation model akin to the Civil Reserve Air Fleet to surge cyber resilience.

Ultimately, it celebrates the tenacity of signal and cyber professionals and invites continued thought leadership that prevents strategic surprise in cyberspace while transforming how the Army teams, trains, and fights in and through a contested homeland.

OPENING

The volatility of today's world requires unceasing diligence in assessing risk to our Army organizations, units, and their missions. Threats in the cyber domain targeting our digital dependencies will always challenge the Army's combat readiness and ability to fulfill peace and wartime missions.

Cyber events like the Colonial Pipeline disruption, and physical events like Hurricane Helene require shared trust and collaboration with commercial and

municipal infrastructure partners that underpin the core functionality of our Army installations and nation. I strongly applaud the Army Cyber Institute at West Point (ACI) for its success in the Jack Voltaic® series of workshops, which have brought much-needed awareness and focus to the complexity of civil-military interdependencies.

I also commend ACI's other invaluable contributions to the Army and operational force, as exhibited by products that make us think critically about how we team and train to tackle our Nation's cyber challenges.

Continued thought leadership is a command imperative if we are to optimize support to the Army's operational force in areas like mission thread defense and national policy analysis. Here, ACI stands at the frontier, on mission to prevent strategic surprise in cyberspace.

To learn more (276 pages):
https://cyberdefensereview.army.mil/Portals/6/Documents/2025-vol10-iss2/CDR_V10_N2_Full_Issue%20VFC.pdf

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.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts. It is our goal to minimize disruption caused by technical errors. However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

Readers that are interested in a specific topic covered in the newsletter, must download the official papers, must find more information, and must ask for legal and technical advice, before making any business decisions.

General Terms and Conditions for all visitors:
https://www.risk-compliance-association.com/Privacy.htm

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.

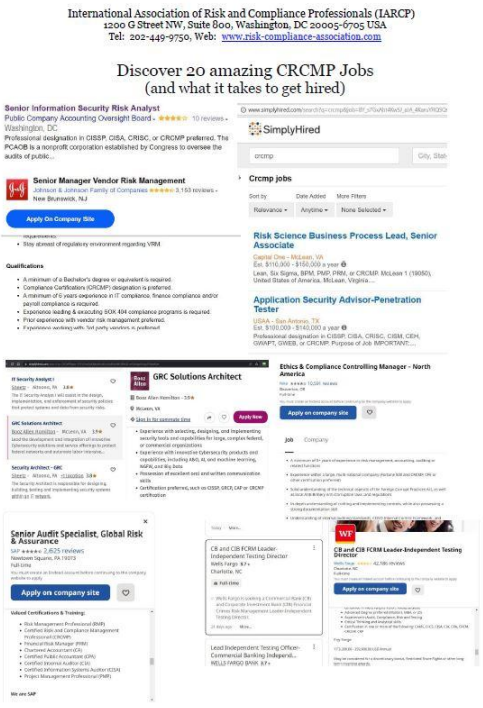
To learn more: https://www.risk-compliance-association.com/Privacy.htm

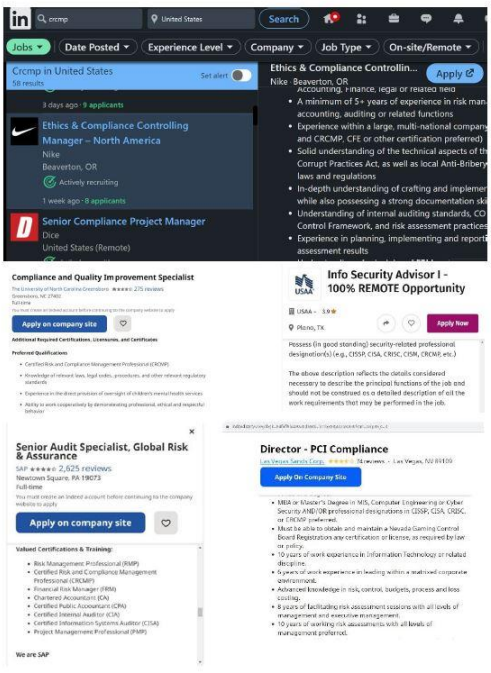
Our training and certification programs:

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(HR²M), online training and certification program. You may visit: https://www.risk-compliance-association.com/CRCMP_HR2M.htm

The CRCMP(HR²M) program is designed to extend the capabilities of CRCMPs into the advanced domains of hybrid risk and resilience. This advanced specialization:

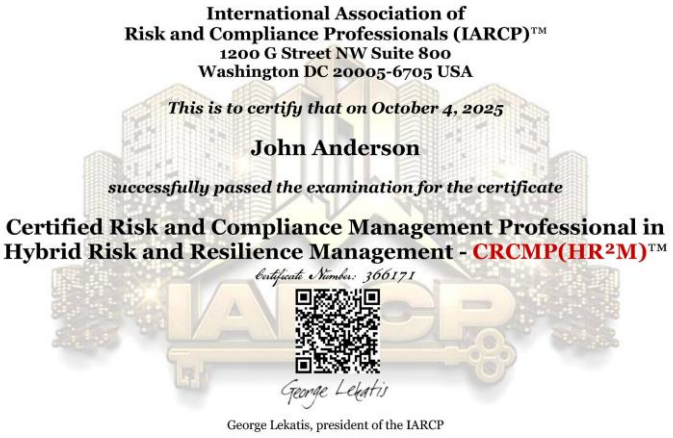
1. Moves from traditional risk and compliance frameworks into the management of multi-vector, cross-domain, and asymmetric threats that transcend conventional boundaries.

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(HR²M) 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

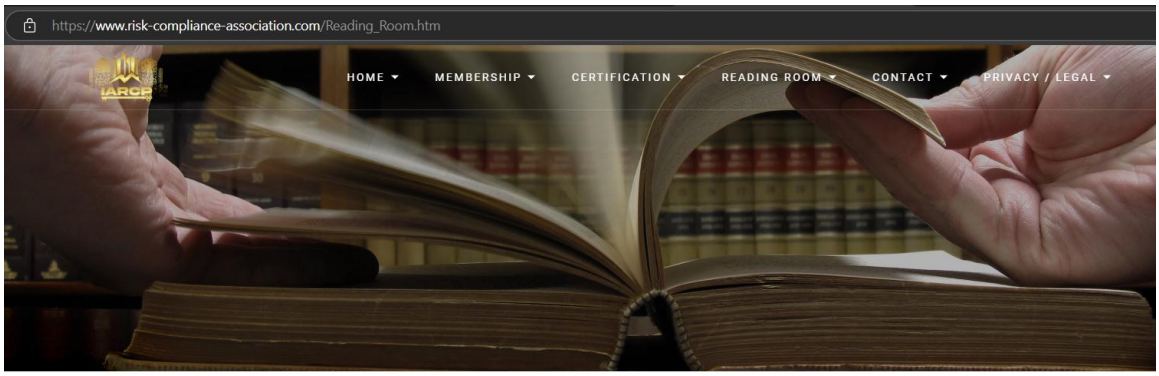
Overview

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