



Monday, February 16, 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.

I was reading the news on my device just after dinner, that quiet hour when markets are closed, inboxes are mercifully silent, and headlines feel less urgent than they did twelve hours earlier. One sentence, however, lingered, impeccably phrased, entirely calm, and clearly aware of the trouble it was not yet announcing.



“Market risks remain **elevated**. Risk related to the **potential** AI bubble **might** boost volatility **without necessarily** default concerns **significantly** increasing.”

In (very) simple terms, markets are still risky. Excitement about AI could make prices swing more, even though companies are not necessarily failing.

In regulatory language, nothing is broken yet, but we are formally paying attention.

A hedge fund manager would read, trade the noise, don't bet on collapse.

“**Elevated**” is one of those words that appears calm, professional, and medically reassuring, as if market risk were a **blood pressure reading** discussed in a well-lit room by people who are not panicking. In plain language, elevated means higher than normal, but not yet high enough to justify urgency, intervention, or raised

voices. It is the **linguistic middle ground** between *everything is fine* and *we should have acted earlier*.

Elevated does not describe a peak, it describes a **persistent condition**. Risk is not spiking, collapsing, or exploding. It is simply... staying up there. Comfortably above baseline. Refusing to come down. Markets are not in distress. They are merely enjoying a higher altitude than usual.

From a regulatory and risk perspective, elevated **signals three things** at once:

- 1. Risk levels are known and measured.** Nothing alarms institutions and investors quite like unmeasured risk. Elevated risk has charts, confidence intervals, and carefully worded explanations.
- 2. Risk is not yet actionable.** Elevated risk does not trigger emergency powers, capital add-ons, or late-night calls. It triggers monitoring, dashboards, and phrases like *continued vigilance*.
- 3. The condition has lasted.** Risk is supposed to fluctuate. When it **remains** elevated, it suggests something structural, behavioral, or narrative-driven rather than cyclical.

There is **elegance** in the word elevated. It recognises that something is wrong, without conceding that anything is weak.

“Risk related to the **potential** AI bubble”. In ordinary language, potential means possible but not certain. In regulatory and risk language, it means something closer to “we are not saying this exists, but we are absolutely saying it could, and we would like that noted.”

The word **potential** is interesting. Calling something an “AI bubble” outright would imply mispricing and collective irrationality. Calling it a potential bubble keeps the door open, and treats the issue as hypothetical, even when behavior suggests otherwise.

This matters because **markets can tolerate discussion of possibilities** far better than statements of diagnosis.

To **experienced readers**, **potential** often signals that early indicators are visible, valuations are decoupling from fundamentals, narratives are leading prices, but confirmation is not yet institutionally comfortable.

I remembered the phrase, *the evidence is suggestive, not yet indictable*.

In law, **suggestive evidence** points toward a possibility. It raises questions. It invites scrutiny. But it does not, by itself, justify formal action, accusation, or enforcement.

Indictable evidence, by contrast, meets a threshold. It is sufficiently robust, corroborated, and attributable to support a charge.

By then it was late, and the news was still coming. [Time, unlike risk](#), had not remained elevated, it had simply moved on.

I put the device aside with the quiet realization that even if markets one day calm down, the flow of carefully worded concern never will. I couldn't help but [admire those who read the news from beginning to end](#).

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(HR²M), online training and certification program.

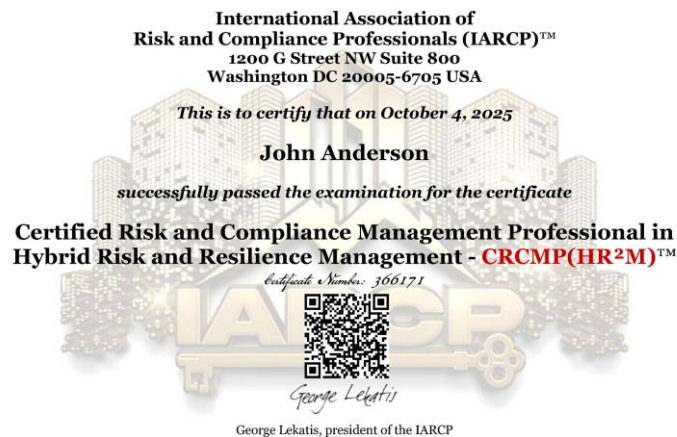
It builds on the solid foundation of the CRCMP designation and equips participants with cutting-edge knowledge to understand, identify, assess, and effectively manage complex hybrid risks.

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)

[Money as a coordination device: some historical lessons](#)

Keynote speech by Mr Hyun Song Shin, Economic Adviser and Head of the Monetary and Economic Department of the BIS, at the 14th ILF Conference on the Future of the Financial Sector.



Number 2 (Page 9)

[The digital euro is an opportunity for Europe](#)

Professor Joachim Nagel, President of the Deutsche Bundesbank
Opening statement at “Bundesbank Spotlight”



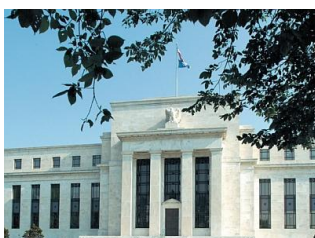
Number 3 (Page 13)

[EIOPA's insurance risk dashboard shows overall stability amidst persistent geopolitical tensions.](#)



Number 4 (Page 16)

[Federal Reserve Board finalizes hypothetical scenarios for its annual stress test and votes to maintain the current stress test-related capital requirements until public feedback can be considered](#)



Number 5 (Page 19)

New PCAOB Publication Provides Auditors With Insights Related to Testing Transactions Between Broker-Dealers and Related Parties



Number 6 (Page 22)

Aiming to protect, with pinpoint precision

Wearable Sandia sensor tracks radiation in real time to better protect cancer patients and warfighters



Number 7 (Page 24)

EU Agencies Network leadership at a time of change in the EU



Number 8 (Page 26)

SUPPLY CHAIN SECURITY



Number 9 (Page 28)

Threat Intelligence - No Place Like Home Network: Disrupting the World's Largest Residential Proxy Network



Number 10 (Page 31)

Subcommittee on **Cybersecurity** - To receive testimony on the Department's cyber force generation plan and the associated implementation plan



Number 1

Money as a coordination device: some historical lessons

Keynote speech by Mr Hyun Song Shin, Economic Adviser and Head of the Monetary and Economic Department of the BIS, at the 14th ILF Conference on the Future of the Financial Sector.



Money is a coordination device that knits together the decisions, plans and obligations of actors in the economy. Common knowledge of the value of money is akin to using a common language.

Once the institution of money takes hold, strong network effects set in motion a virtuous circle between greater acceptance and greater use. The more others accept and use a particular form of money, the more I wish to adopt it too.

Central banks historically have served as the lightning rod for the coordinated acceptance of money.

How do cryptoassets and stablecoins fare in this context? Rather than coalescing around a single platform, the crypto ecosystem has become increasingly fragmented, not only in the underlying "layer 1" blockchains, but also in the so-called "layer 2" blockchains that build on top of the underlying layer.

Rather than coordination and network effects that spring from the virtuous circle of greater use and greater acceptance, we see the increasing fragmentation of crypto and the infrastructure ("the rails") that supports it.

Why does crypto lead to greater fragmentation?

The decentralisation agenda that underpins crypto rejects centralised trust in favour of dispersed validators achieving consensus through token economics, or "tokenomics", which underpins the actions of the validators themselves.

The validators need sufficient rewards to play their allotted role in the governance of the blockchain. Rewards are in the form of user fees, or other benefits that come from deciding on the sequence of transactions to take place on the blockchain. To sustain validator incentives, congestion and capacity constraints are necessary.

When more users flock to a particular blockchain, the capacity constraints become a deterrent for new users to join. Rather than the virtuous circle of greater acceptance and greater use, there is greater fragmentation through the emergence of new blockchains to cater to the users who turn away from existing blockchains. Fragmentation undermines the network effects of money.

This presentation explores the implications of these structural forces behind the institution of money, emphasising the trade-offs between decentralisation and the coordination role of money. It examines how fragmentation affects the functioning of the monetary system and raises critical questions for its future. For a monetary system where stablecoins play a significant role, the design of the points of contact between stablecoins and the conventional monetary system emerges as a key feature for future work.

Ultimately, the presentation underscores the enduring importance of trust, coordination, and policy innovation in navigating the future of money.

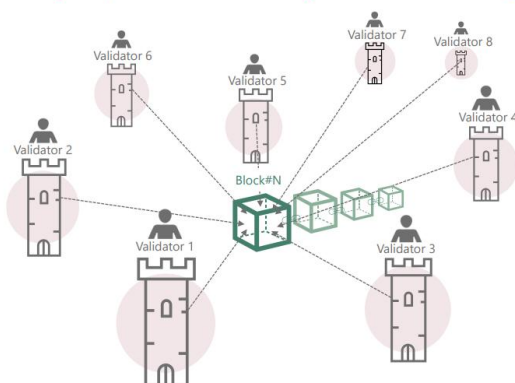
History holds lessons on the role of the central bank in the monetary system; the Bank of Amsterdam (1609-1820) is a good example



BIS

2

The decentralisation agenda rejects a centralised notion of trust (eg, provided by central banks); money depends on achieving consensus among dispersed validators



BIS

8

To learn more: <https://www.bis.org/speeches/sp260127.htm>



*Number 2***The digital euro is an opportunity for Europe**

Professor Joachim Nagel, President of the Deutsche Bundesbank
Opening statement at “Bundesbank Spotlight”

*1 Introductory remarks*

Ladies and gentlemen,
Welcome to the first Bundesbank Spotlight in Berlin!

What is the idea behind the new event format? We want to engage in personal dialogue with experts in their fields and with our guests.

The focus of our first Spotlight will be the digital euro. For this event, we have invited two guests to the podium, and I am delighted that they are able to be here today: Ramona Pop from the Federation of German Consumer Organisations, and Christian Sewing – who will engage in today’s discussion not only in his capacity as CEO of Deutsche Bank but also as President of the Association of German Banks.

By introducing the digital euro, we want to make our single currency, the euro, fit for the future. Our vision is to create a single European payment solution that is state of the art in terms of technology, enables innovation, makes Europe more independent and resilient, and is trustworthy.

In the current project phase, we are preparing to be able to issue the digital euro in the course of 2029. We assume that the legal framework for the digital euro will be in place by the end of this year. This legal basis is a prerequisite for the Eurosystem to be able to start issuing the digital euro.

We are working closely with policymakers and banks. They will be a crucial interface between users of the digital euro and the Eurosystem as its issuer. We are already in close dialogue with the general public and, through many events across the country, are clarifying what the digital euro is and what it is not – what benefits it will offer and how data protection and security will be ensured, for instance.

According to a Forsa survey conducted on behalf of the Bundesbank, only 42 % of survey participants had heard or read about the digital euro in October 2025. And only just over one-quarter of them knew what it is: an additional digital means of payment issued by the Eurosystem. This shows that we have a considerable amount of work to do to educate the general public.

2 The benefits of the digital euro

The digital euro will enable cashless payments to be made simply, securely and across borders throughout the euro area.

The digital euro will be just as trustworthy as our banknotes and coins. It is intended to be a digital supplement, a digital “twin” to euro cash, and not a substitute.

You would be able to use it just as easily as your girocard and existing payment apps on your smartphone – be it at a point of sale, in a restaurant, when shopping online or for credit transfers to friends. And it will also be able to be used offline. No other means of payment apart from the digital euro offers all these features at once in the euro area.

The digital euro also presents an opportunity to overcome the strong fragmentation of the European payments market. At present, there is no European payment solution that is accepted in all euro area countries – except for cash.

Instead, non-European providers, particularly from the United States, dominate the market. These providers often charge retailers high fees, which we as consumers ultimately pay, too.

I’m sure you are familiar with the film “Pretty Woman”. Then you might remember the quote “Stores are never nice to people, they’re nice to credit cards”. The truth, however, is that while retailers accept credit cards and online payment services, they often do so only reluctantly because of the high fees.

By contrast, the digital euro will be a cost-effective alternative to existing digital means of payment for retailers. This is another reason why the retail sector is very open to the digital euro. After all, it will stimulate competition in the payment market.

Critics, on the other hand, complain that this would cut the ground from under the feet of private sector initiatives for a European payment solution. But, the opposite is true: private sector solutions such as Wero could benefit from the pan-European reach of the digital euro, for example by integrating the digital euro into the Wero wallet. On the flip side, Wero could be an important means by which people use the digital euro – a win-win situation!

I am also convinced that the market offers sufficient space for private and public sector providers. This is because consumers also appreciate the possibility of being able to choose between different options.

The digital euro is also being designed to enable future innovations and functions. I am thinking, for instance, of conditional payments: a parcel only being paid for when the customer receives it, to name one example, or a travel refund being issued automatically if a train is delayed, to name another.

Launching the digital euro also means we are increasing our strategic autonomy – something which is unfortunately desperately needed in view of geopolitical developments.

Visa and Mastercard currently account for almost two-thirds of all card payments in the euro area. 13 out of 21 euro area countries do not have an own national card system like we have girocard in Germany.

These countries therefore rely entirely on non-European card systems, including within their own country's borders. To put it bluntly, we are very dependent on US corporations in payments today – too dependent.

Payments are part of our critical infrastructure. And we really ought to stand on our own two feet when it comes to critical infrastructure. The digital euro would be the first and only digital means of payment built on a European infrastructure that could be used seamlessly throughout the euro area.

And what about data protection?

To protect your data, we are designing the digital euro to offer the highest degree of privacy possible for an electronic means of payment. Privacy has been a top priority of the digital euro project since its inception. The Eurosystem central banks will not be able to tell who is behind individual payments.

We certainly will not be able to and do not want to control what the public pay for with the digital euro. And those who use the digital euro offline will pay almost as anonymously as they do with cash.

Many people are not even aware of how much data they share when paying using other digital means of payment. For some people it does not matter. However, we know from surveys that protecting privacy is a crucial factor for many consumers. According to the Forsa survey I mentioned earlier, it would represent the most important feature for 74 % of respondents.

3 Conclusion

Ladies and gentlemen,
I am convinced that the digital euro will be a success.

It is up to us to bring the euro to where a great future lies ahead of it: the digital world.

The digital euro stands for payments that are simple, secure and European – open to innovation, regardless of external factors, and trustworthy for all.

We want to develop the digital euro together with consumers, banks, retailers and policymakers.

It is neither a project opposing cash, nor a project opposing private sector providers.

It is a project of progress for our continent's population.

The digital euro is an opportunity for Europe.

Thank you for listening.

To learn more:

<https://www.bundesbank.de/en/tasks/topics/professor-nagel-at-bundesbank-spotlight-the-digital-euro-is-an-opportunity-for-europe--987786>



*Number 3***EIOPA's insurance risk dashboard shows overall stability amidst persistent geopolitical tensions.**

The European Insurance and Occupational Pensions Authority (EIOPA) published its January 2026 Insurance Risk Dashboard. The main findings show that risks in the European insurance sector remain stable at a medium level, amidst an uncertain geopolitical environment weighing on the macroeconomic and market risk outlook.

January 2026 Insurance Risk Dashboard

Risks	Level	Trend (Past 3 months)	Outlook (Next 12 months)
Macro risks	Yellow	→	↗
Credit risks	Yellow	→	→
Market risks	Orange	→	→
Liquidity & funding risks	Yellow	↗	→
Profitability & solvency risks	Yellow	→	→
Interlinkages & imbalances risks	Yellow	→	→
Insurance risks	Yellow	↘	→
Market perceptions	Yellow	→	→
ESG related risks	Yellow	↘	→
Digitalisation & cyber risks	Yellow	→	→

The reference date for company data is Q3-2025 for quarterly indicators and 2024-YE for annual indicators. The cut-off date for most market indicators is the end of December 2025. The Level (color) corresponds to the level of risk as of the reference date, the Trend is displayed for the 3 months preceding the reference date and the Outlook is displayed for the 12 months after the reference date. The latter is based on the responses received from 23 national competent authorities (NCAs) and ranked according to the expected change in the materiality of each risk (substantial decrease, decrease, unchanged, increase and substantial increase).

The macroeconomic environment remains stable at a medium level, supported by continued GDP growth, easing inflation.

However, persistent and widening geopolitical tensions—most notably involving Venezuela, Iran, and emerging frictions around Greenland—are increasing uncertainty and rendering the outlook for trade, energy, and security increasingly complicated. At the same time, higher public spending needs, particularly for defence and infrastructure, may constrain fiscal space over the medium term.

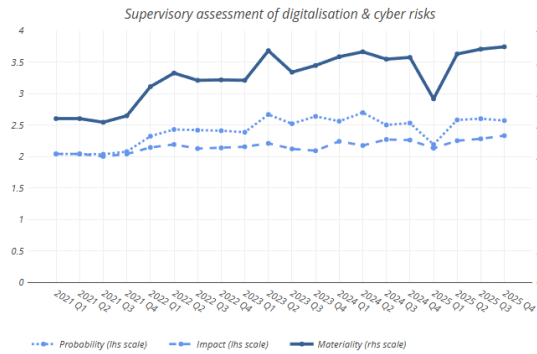
Financial markets remain vulnerable to valuation pressures, with indicators continuing to point to potential detachment from fundamentals. While recent increases in volatility have been contained, the potential unwinding of an AI-related asset price bubble could amplify market fluctuations, even if this does not immediately translate into higher default risk.

Credit and liquidity conditions remain broadly stable, though funding dynamics show early signs of pressure amidst increased issuance and sustained refinancing needs.

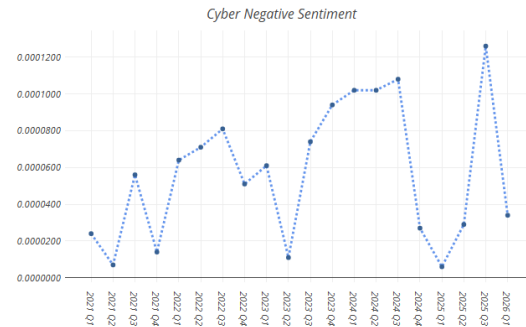
The insurance sector continues to demonstrate resilience, supported by solid capital positions, stable profitability, and strong premium growth. Credit and liquidity conditions remain broadly stable. Nonetheless, geopolitical tensions, trade disruptions, and cyber events call for continued vigilance.

Digitalisation & cyber risks

Digitalization and cyber risks remain at a medium level. The materiality of these risks for the insurance sector, as assessed by supervisors, remain elevated in Q4 2025. Cyber negative sentiment and global cyber attacks indicators decreased at the end of 2025. In the current geopolitical context, cyber threats remain significant concern as insurers are not only exposed to operational risks but also face the growing challenge of underwriting cyber risks, which adds complexity to their risk management strategies.



Note: Scores compiled based on the assessment of probability and impact (lhs scale from 1 to 4) of digitalisation & cyber risks from National Competent Authorities. The country average for each answer is then normalised (rhs scale 0-100). Source: EIOPA's Insurance Bottom-up Survey.



Note: Text analysis based indicator, calculated from earning calls transcripts from listed insurers. Source: Refinitiv, EIOPA calculations.

Background

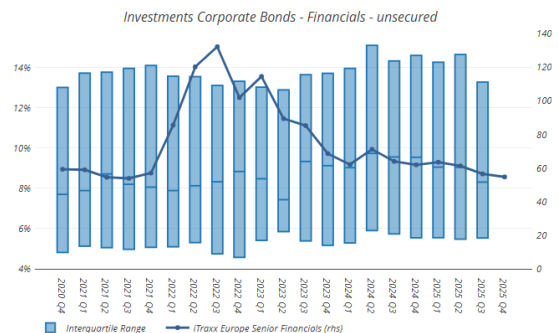
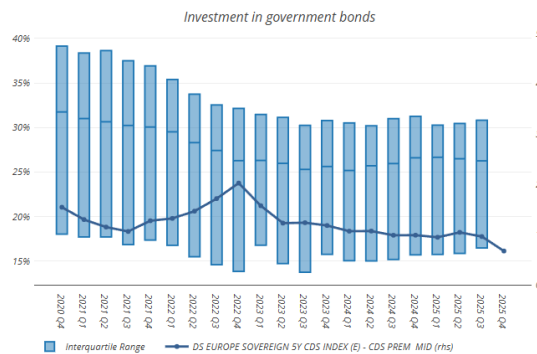
This Insurance Risk Dashboard, based on Solvency II data, summarises the main risks and vulnerabilities in the European insurance sector through a set of risk indicators from the third quarter of 2025 and end-2024.

The data is based on financial stability and prudential reporting collected from 97 insurance groups and 2124 solo insurance undertakings.

The Solvency II information is complemented with market data with cut-off date end-December 2025.

Credit Risks

Credit risks remain steady at a medium level, foreseen increase in public spending in defense and infrastructure. As of end of December 2025, credit default swap (CDS) spreads decreased slightly. In Q3 2025, insurers' median exposures to government and financial bonds remained broadly unchanged, while their exposures to non-financial bonds decreased. As of Q3 2025, insurers' median investment allocations as a share of total assets stood at approximately 26.3% in government bonds, at 1.3% in financial secured bonds and slightly decreased to 8.3% in financial unsecured bonds and decreased to 8.7% from 10.4% in non-financial bonds. The indicator on fundamental credit risk in the non-financial corporate sector was broadly unchanged. Insurers' exposure to mortgages and loans remained around 0.3% in Q3-2025 and the household debt-to-income ratio in the Euro area declined slightly to 82.7%, based on Q1 2025 data. Overall, the credit quality of insurers' investments remains high, with the median credit quality step (CQS) around 2, equivalent to an AA rating from S&P. The median share of low-rated investments (CQS > 3) was around at 1.3% in Q3 2025.



To learn more:

https://www.eiopa.europa.eu/eiopas-insurance-risk-dashboard-shows-overall-stability-amidst-persistent-geopolitical-tensions-2026-01-30_en



Number 4

Federal Reserve Board finalizes hypothetical scenarios for its annual stress test and votes to maintain the current stress test-related capital requirements until public feedback can be considered



The Federal Reserve Board finalized the [hypothetical scenarios](#) for its annual stress test, which helps ensure that large banks can continue to lend to households and businesses even in a severe recession. The final scenarios are substantially similar to the scenarios proposed in [October](#).

October 24, 2025

Federal Reserve Board requests comment on proposals to enhance the transparency and public accountability of its annual stress test

For release at 3:30 p.m. EDT

Share 

Consistent with its prior statement, the Federal Reserve Board on Friday requested comment on proposals to enhance the transparency and public accountability of its annual stress test. The proposals seek comment on: the stress test models; changes to the framework that guides the design of the hypothetical scenarios; and the hypothetical scenarios for the upcoming 2026 stress test.

Additionally, the Board voted to [maintain the current stress capital buffer requirements until 2027](#), when new requirements can be calculated based on models that take public feedback into consideration.

"Waiting to calculate new stress capital buffer requirements until we receive public feedback will give us the opportunity to correct any deficiencies in our supervisory models based on that feedback," said Vice Chair for Supervision Michelle W. Bowman. "This should further improve the transparency, effectiveness, and fairness of our models and improve our accountability to the public."

The Board's annual stress test evaluates the resilience of large banks by estimating losses, net revenue, and capital levels under hypothetical recession scenarios that extend two years into the future. This year, 32 banks will be tested against a severe global recession with heightened stress in both commercial and residential real

estate markets, as well as in corporate debt markets. The scenarios are not forecasts and should not be interpreted as predictions of future economic conditions.

In the 2026 stress test scenario, the U.S. unemployment rate rises nearly 5.5 percentage points, to a peak of 10 percent. The unemployment rate increase is accompanied by severe market volatility, a widening of corporate bond spreads, and a collapse in asset prices, including about a 30 percent decline in house prices and a 39 percent decline in commercial real estate prices.

Large banks with substantial trading or custodial operations are also required to incorporate a counterparty default scenario component to estimate potential losses from the unexpected default of the firm's largest counterparty amid an acute market shock.

In addition, banks with large trading operations will be tested against a global market shock component that primarily stresses their trading and related positions. The final scenarios include two revisions to the global market shock component to improve consistency across shocks applied to similar exposures and enhance plausibility.

The table below shows the components of the annual stress test that apply to each bank, based on data as of the third quarter of 2025. The brief methodology document describes the Board's intention to generally use the same models as the 2025 stress test with limited model adjustments.

Bank ¹	Subject to global market shock	Subject to counterparty default
Ally Financial Inc.		
American Express Company		
Bank of America Corporation	x	x
The Bank of New York Mellon Corporation		x
Barclays US LLC	x	x
BMO Financial Corp.		
Capital One Financial Corporation		
The Charles Schwab Corporation		
Citigroup Inc.	x	x
Citizens Financial Group, Inc.		
DB USA Corporation	x	x
Fifth Third Bancorp		

First Citizens Bancshares, Inc.		
The Goldman Sachs Group, Inc.	x	x
HSBC North America Holdings Inc.		
Huntington Bancshares Incorporated		
JPMorgan Chase & Co.	x	x
KeyCorp		
M&T Bank Corporation		
Morgan Stanley	x	x
Northern Trust Corporation		
The PNC Financial Services Group, Inc.		
RBC US Group Holdings LLC		
Regions Financial Corporation		
Santander Holdings USA, Inc.		
State Street Corporation		x
Synchrony Financial		
TD Group US Holdings LLC		
Truist Financial Corporation		
UBS Americas Holding LLC		
U.S. Bancorp		
Wells Fargo & Company	x	x

To learn more:

<https://www.federalreserve.gov/newsevents/pressreleases/bcreg20260204a.htm>



*Number 5***New PCAOB Publication Provides Auditors With Insights Related to Testing Transactions Between Broker-Dealers and Related Parties**

The PCAOB released a staff publication, “Broker-Dealer Audit Focus: Related Party Transactions.”

Under federal law, the PCAOB has the responsibility to oversee firms that audit broker-dealers registered with the U.S. Securities and Exchange Commission.

PCAOB staff continues to identify deficiencies related to the testing of transactions between brokers and dealers and related parties (typically parents or affiliates). This edition of Broker-Dealer Audit Focus highlights key reminders for auditors of broker-dealers from PCAOB standards related to audit procedures involving a broker-dealer’s revenue and expense transactions with related parties. It also provides the staff’s perspective on common deficiencies observed in broker-dealer inspections and shares good practices that the staff has observed.



AS 2410, Related Parties (“AS 2410”), states that the auditor’s objective is to obtain sufficient appropriate audit evidence to determine whether related parties and relationships and transactions with related parties have been properly identified, accounted for, and disclosed in the financial statements.

To meet these objectives, the auditor:

- Performs risk assessment procedures to obtain an understanding of the broker-dealer’s relationships and transactions with its related parties.
- Identifies and assesses the risks of material misstatement associated with relationships and transactions with the broker-dealer’s related parties.

- Responds to the risks of material misstatement.
- Evaluates whether the broker-dealer has properly identified relationships and transactions with its related parties.
- Evaluates the financial statement accounting for and disclosure of the relationships and transactions between the broker-dealer and its related parties.
- Communicates to the audit committee (or its equivalent) the auditor's evaluation of the broker-dealer's identification of, accounting for, and disclosure of relationships and transactions with its related parties.

Common Deficiencies

The following are some of the common deficiencies that the staff has observed in the testing by audit firms of transactions between a broker-dealer and its parent or affiliates:



Not testing the allocation of revenues and expenses

between a broker-dealer and its parent or affiliates, including the accuracy and completeness of information used in the allocation.



Not evaluating whether allocated revenues or expenses are consistent

with the terms of the written agreements between the broker-dealer and its parent or affiliates.

Not evaluating the financial capability

of a broker-dealer's parent or affiliates to satisfy a material uncollected balance owed to the broker-dealer.



Not identifying omitted or inaccurate disclosures

in the broker-dealer's financial statements necessary to understand the effects of transactions between a broker-dealer and its parent or affiliates.



Not communicating to the audit committee

(or its equivalent) the auditor's evaluation of the broker-dealer's identification of, accounting for, and disclosure of transactions with its parent or affiliates.



Good Practices

The following good practices may assist audit firms who audit broker-dealers with the testing of transactions between a broker-dealer and its parent or affiliates:



Practice Aid

Use of a practice aid that contains guidance to assist engagement teams with (1) understanding the broker-dealer's relationships and transactions with its related parties that includes the broker-dealer's process for identification, authorization, accounting, and disclosure of related party transactions, (2) performing inquiries of management, others at the broker-dealer, and the audit committee (or its equivalent), and (3) responding to the identified risks of material misstatement, including guidance for testing of allocated revenues and expenses.

Checklists

Use of financial statement disclosure and audit committee communication checklists identifying the required financial statement disclosures and communications for the audit committee (or its equivalent).



Training

Training audit personnel on the requirements of AS 2410 and FASB ASC Topic 850, as well as the industry-specific requirements of FINRA Notice to Members 03-63 and related audit considerations for broker-dealers with management service, expense sharing, or similar agreements.



To learn more:

https://assets.pcaobus.org/pcaob-dev/docs/default-source/documents/bd-audit-focus-related-party-transactions.pdf?sfvrsn=cb8ef7ac_1



Number 6

[Aiming to protect, with pinpoint precision](#)

Wearable Sandia sensor tracks radiation in real time to better protect cancer patients and warfighters



A new wearable patch to help protect cancer patients and American warfighters from harmful radiation has been developed by a small team of Sandia National Laboratories researchers. The disposable sensor is designed to be worn on the skin or clothes and produced at scale.

Sandia researchers Patrick Doty and Isaac Aviña developed the wearable dosimeter that could change the way radiation therapy is administered by providing real-time feedback on radiation delivery and improving treatment accuracy. Combining advanced light-sensing polymers and microelectronic grids, the team used a state-of-the-art in-house developed laser etching machine at Sandia's California site to create thousands of disposable patches.

“Right now, in the medical world, we aim beams at cancerous cells with a wide range of error,” Aviña said. “That means sometimes we leave large parts of cancerous cells and other times we hit healthy tissue. To fix this problem, we need better accuracy.”

This need is particularly acute for children. A 2022 National Institutes of Health study found that it is difficult to ensure radiation goes only where it is needed and that “children are particularly susceptible to late adverse effects of radiation.”

“They know exactly what the beam current is and what the energy is, so they know exactly where it's going in XY space and where it's going to stop in a tank of water,” Doty said. “But what they don't know is where the patient is. They might breathe or move.”

The new dosimeter not only measures radiation dose but can also alert clinicians if the radiation is off target. The patch includes a polymer that interacts with radiation in real time, allowing it to track both the location and dosage of radiation as it passes through the patient. If the patient moves, the system can react instantly, shutting off the beam to help prevent harm to healthy tissue.

The technology is licensed to Virginia company WearableDose Inc., which earned top global Innovation of the Year honors at the MedTech World Awards in November 2025.

The research team is now receiving funding from the Defense Threat Reduction Agency to explore how the patches can enhance situational awareness and monitor exposure for military personnel in hazardous environments. This work translates to improving military readiness and long-term health outcomes for today's warfighters.

As the team continues to refine their technology, they remain motivated by personal experiences with cancer and the desire to improve patient care.

“Everybody should want to do something about this,” Doty said.

To learn more: <https://newsreleases.sandia.gov/dosimeter-patch>



Number 7

EU Agencies Network leadership at a time of change in the EU



As Chair of the EU Agencies Network (EUAN) 2025-2026, ENISA pursued key priorities on implementing the new governance framework of the network, it asserted the role of Agencies as key institutional partner and strengthened cybersecurity across the EU Agencies and Joint Undertakings, leading to greater efficiency through sharing services.

Bringing together 52 EU Agencies and Joint Undertakings, EUAN supports over 14,000 staff located across almost all Member States covering many portfolios. In the first week of February 2026, Agency Directors and leaders on resources and human resources alike joined topical coordination meetings in Athens to discuss ways to respond to challenges at a time of change for the EU. These events brought together the Heads of Agency Directors, Heads of Resources and Heads of Human Resources.

Efficient public management by means of Shared Services

On the sidelines of the Heads of Agencies meeting, the Directors of European Institute of Innovation and Technology (EIT), European Food Safety Authority (EFSA) and ENISA signed a Memorandum of Understanding (MoU) to reassert cooperation on shared services that had previously been launched as a pilot.

Shared Services have long been scoped and the latest iteration of the pilot in 2026 focuses on selected HR services, cybersecurity compliance, preparedness and response, as well as legal services. The pilot established an operational framework, with a view to bringing about concrete change and to consolidating the experience acquired.

A valued institutional partner

During its term at the coordination help, ENISA proactively interacted with selected EU Institutions including European Commission, European Parliament and the Council of the European Union, as well as with the European Court of Auditors, and other stakeholders as appropriate.

Member of the European Parliament Mr. Hélder Sousa Silva, Standing Rapporteur of the European Parliament BUDG Committee, visited ENISA's headquarters for a bilateral exchange with the Executive Director and senior management.

The meeting built on the dialogue launched at the EU Agencies Network (EUAN) Heads of Agencies meeting in February 2025, where he joined as a guest speaker

on the next EU long-term budget, the Multiannual Financial Framework 2028-2034, which heralds EU policy change at a scale.

During his visit to ENISA, MEP Sousa Silva underlined his commitment to work closely with de-centralised Agencies and Joint Undertakings and highlighted the need to balance longstanding EU priorities with emerging ones, while ensuring greater flexibility and cutting unnecessary red tape.

ENISA, has led close collaboration with the European Commission on key HR priorities - encouraging staff performance, attracting and retaining talent, and fostering inclusive workplaces while addressing challenging topics, including aspects of recruitment, staff management and teleworking and financial planning.

Alongside collaboration on increasing efficiency and better resource planning, the focus of the inter-institutional cooperation was on the next Multiannual Financial Framework. These exchanges helped connect policies' priorities with the concrete ways to deliver tangible results.

Supporting an enhanced cybersecurity

In an effort to step up on user awareness, making available tools and methods to strengthen cybersecurity across EU Agencies and Joint Undertakings has been a standing priority of the ENISA EUAN Chair. In this vein, ENISA supports Agencies in improving cybersecurity preparedness and thus, helps them comply with EU compliance requirements. In the plenary meeting in Athens, gamification in cybersecurity let Agencies' Directors come to terms with the challenges that cybersecurity response is all about.

EU Agencies Network

The role of the EUAN is to enable structured collaboration across EU decentralised Agencies and Joint Undertakings to drive innovation, enhance efficiency, and strengthen Europe's competitiveness. Through closer cooperation, EUAN members deliver better services and build a smarter, safer Europe that meets the needs of all citizens.

EUAN is led by a Steering Board (SB) which in 2025 was composed of the Directors of EIT, CEPOL, ELA, SESAR JU, CPVO as well as Pillar Coordinators from EEA, EFSA, F4E and later CdT; in 2025-26, ENISA chaired the EUAN SB. The EUAN Shared Services Office supports a broad range of cost-effective services to EUAN Board and the Network as a whole.

ENISA has been grateful to all stakeholders for their enthusiasm to contribute to EUAN, be constructive in the face of change and strengthen the EU further. Our wishes for success go to ELA, the incoming Chair of EUAN in the next term.

To learn more:

<https://www.enisa.europa.eu/news/eu-agencies-network-leadership-at-a-time-of-change-in-the-eu>

Number 8

SUPPLY CHAIN SECURITY



United States Government Accountability Office
Report to Congressional Committees

Overview of Key Points in the Global Cargo Supply Chain

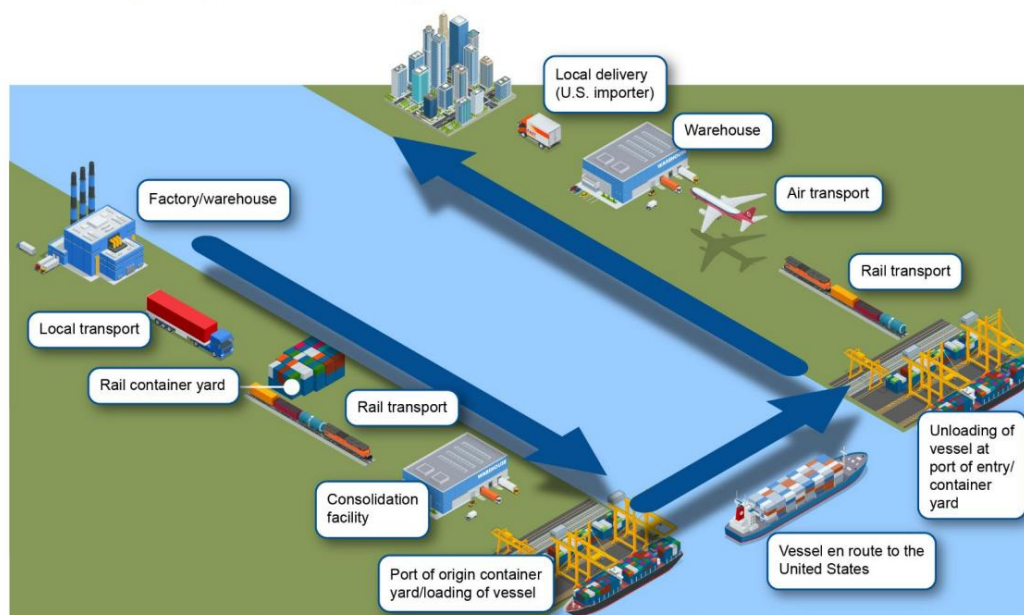
The global supply chain consists of multiple key points of transfer from the time that a shipment is loaded with goods at a foreign factory to when it arrives at a U.S. port and ultimately is delivered to the end user.

For example, air cargo's movement depends on warehouses, trucks, roadways, and other ground-based infrastructure at and around airports, while transporting a shipping container involves many different participants and many points of transfer, such as facilities, vessels, and infrastructure within seaports.

In the post-9/11 environment, the movement of cargo shipments throughout the global supply chain is inherently vulnerable to terrorist actions. Every time responsibility for cargo shipments changes hands along the global supply chain, there is the potential for a security breach.

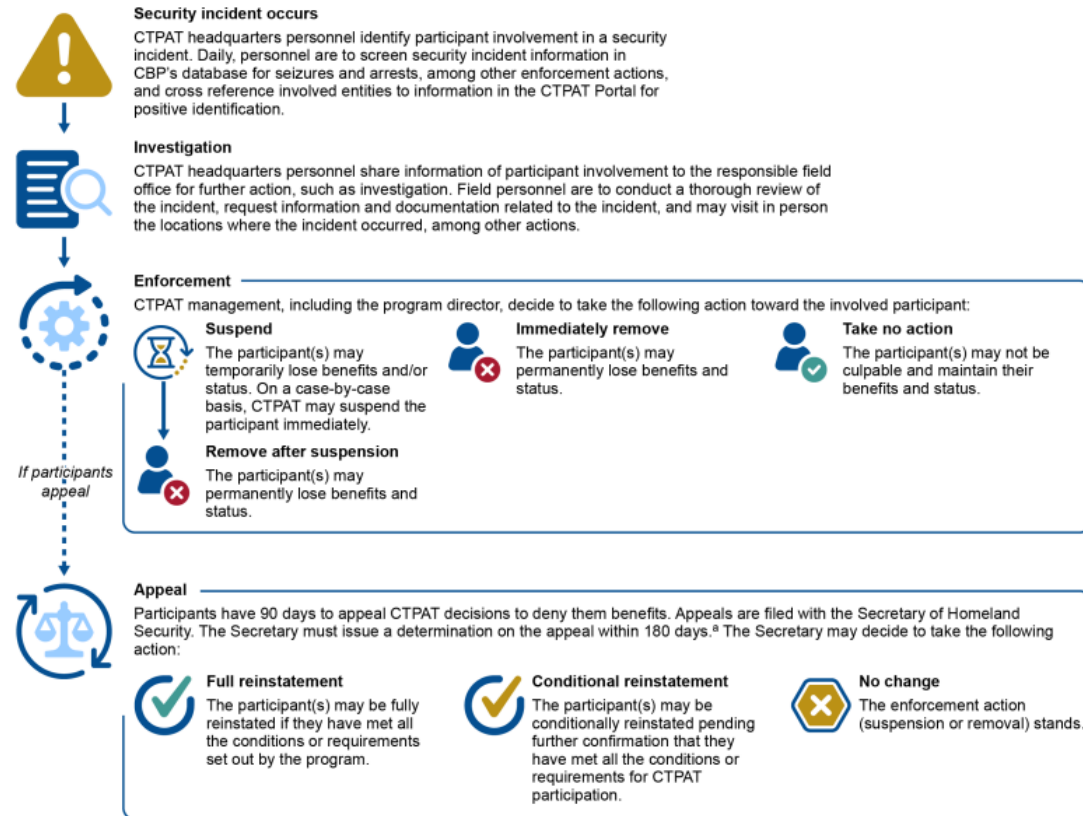
For example, the cargo in a shipping container can be affected not only by the manufacturer or supplier of the material being shipped, but also by carriers who are responsible for getting the material to a port and by personnel who load containers onto the ships. Thus, vulnerabilities exist that terrorists could exploit by, for example, placing a weapon of mass destruction into a container for shipment to the United States or elsewhere. See figure 1 for an example of the global supply chain.

Figure 1: Example of Key Points in the Global Supply Chain



Source: GAO analysis of U.S. Customs and Border Protection information; Golden Sikorka/stock.adobe.com (illustrations). | GAO-26-107893

Figure 5: Overview of U.S. Customs and Border Protection's (CBP) Process for Addressing Customs Trade Partnership Against Terrorism (CTPAT) Participant Involvement in Security Incidents



Source: GAO analysis of CBP documents and relevant legislation; Icons-Studio/stock.adobe.com. | GAO-26-107893

Note: Our analysis included CTPAT operating procedure documents and Pub. L. No. 109-347, tit. II, subtit. B, §§ 211-23, 120 Stat. 1884, 1909-15 (codified at 6 U.S.C. §§ 961-73).

⁸6 U.S.C. § 967(c)(1).

To learn more: <https://www.gao.gov/assets/gao-26-107893.pdf>



Number 9

Threat Intelligence - No Place Like Home Network: Disrupting the World's Largest Residential Proxy Network



Google and partners took action to disrupt what we believe is one of the largest residential proxy networks in the world, the IPIDEA proxy network. IPIDEA's proxy infrastructure is a little-known component of the digital ecosystem leveraged by a wide array of bad actors.

This disruption, led by Google Threat Intelligence Group (GTIG) in partnership with other teams, included three main actions:

- Took legal action to take down domains used to control devices and proxy traffic through them.
- Shared technical intelligence on discovered IPIDEA software development kits (SDKs) and proxy software with platform providers, law enforcement, and research firms to help drive ecosystem-wide awareness and enforcement. These SDKs, which are offered to developers across multiple mobile and desktop platforms, surreptitiously enroll user devices into the IPIDEA network. Driving collective enforcement against these SDKs helps protect users across the digital ecosystem and restricts the network's ability to expand.
- These efforts to help keep the broader digital ecosystem safe supplement the protections we have to safeguard Android users on certified devices. We ensured Google Play Protect, Android's built-in security protection, automatically warns users and removes applications known to incorporate IPIDEA SDKs, and blocks any future install attempts.

We believe our actions have caused significant degradation of IPIDEA's proxy network and business operations, reducing the available pool of devices for the proxy operators by millions. Because proxy operators share pools of devices using reseller agreements, we believe these actions may have downstream impact across affiliated entities.

Dizzying Array of Bad Behavior Enabled by Residential Proxies

In contrast to other types of proxies, residential proxy networks sell the ability to route traffic through IP addresses owned by internet service providers (ISPs) and used to provide service to residential or small business customers.

By routing traffic through an array of consumer devices all over the world, attackers can mask their malicious activity by hijacking these IP addresses. This generates significant challenges for network defenders to detect and block malicious activities.

A robust residential proxy network requires the control of millions of residential IP addresses to sell to customers for use. IP addresses in countries such as the US, Canada, and Europe are considered especially desirable.

To do this, residential proxy network operators need code running on consumer devices to enroll them into the network as exit nodes. These devices are either pre-loaded with proxy software or are joined to the proxy network when users unknowingly download trojanized applications with embedded proxy code.

Some users may knowingly install this software on their devices, lured by the promise of “monetizing” their spare bandwidth. When the device is joined to the proxy network, the proxy provider sells access to the infected device’s network bandwidth (and use of its IP address) to their customers.

While operators of residential proxies often extol the privacy and freedom of expression benefits of residential proxies, Google Threat Intelligence Group’s (GTIG) research shows that these proxies are overwhelmingly misused by bad actors.

IPIDEA has become notorious for its role in facilitating several botnets: its software development kits played a key role in adding devices to the botnets, and its proxy software was then used by bad actors to control them. This includes the BadBox2.0 botnet we took legal action against last year, and the Aisuru and Kimwolf botnets more recently.

We also observe IPIDEA being leveraged by a vast array of espionage, crime, and information operations threat actors. In a single seven day period in January 2026, GTIG observed over 550 individual threat groups that we track utilizing IP addresses tracked as IPIDEA exit nodes to obfuscate their activities, including groups from China, DPRK, Iran and Russia. The activities included access to victim SaaS environments, on-premises infrastructure, and password spray attacks.

Our research has found significant overlaps between residential proxy network exit nodes, likely because of reseller and partnership agreements, making definitive quantification and attribution challenging.

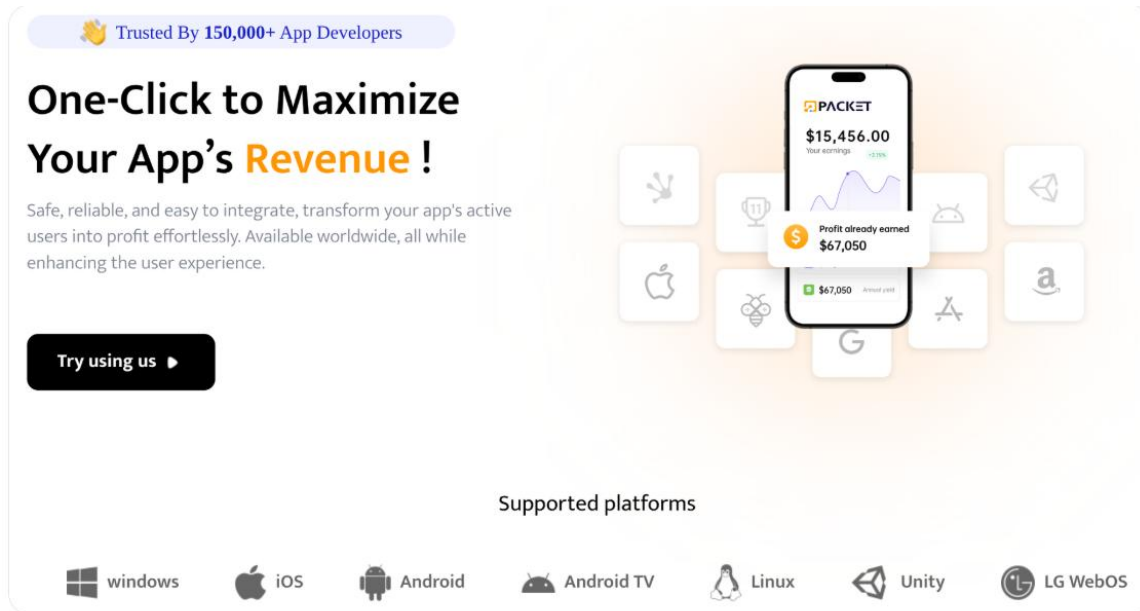
In addition, residential proxies pose a risk to the consumers whose devices are joined to the proxy network as exit nodes. These users knowingly or unknowingly provide their IP address and device as a launchpad for hacking and other unauthorized activities, potentially causing them to be flagged as suspicious or blocked by providers.

Proxy applications also introduce security vulnerabilities to consumers’ devices and home networks. When a user’s device becomes an exit node, network traffic that they do not control will pass through their device.

This means bad actors can access a user’s private devices on the same network, effectively exposing security vulnerabilities to the internet. GTIG’s analysis of these applications confirmed that IPIDEA proxy did not solely route traffic

through the exit node device, they also sent traffic to the device, in order to compromise it.

While proxy providers may claim ignorance or close these security gaps when notified, enforcement and verification is challenging given intentionally murky ownership structures, reseller agreements, and diversity of applications.



The image is a screenshot of a web advertisement for PacketSDK. At the top left, it says "Trusted By 150,000+ App Developers" with a gold star icon. The main headline is "One-Click to Maximize Your App's Revenue!". Below this, a sub-headline reads: "Safe, reliable, and easy to integrate, transform your app's active users into profit effortlessly. Available worldwide, all while enhancing the user experience." A black button with white text says "Try using us ▶". To the right, a smartphone displays the PacketSDK interface with a balance of \$15,456.00 and a profit of \$67,050. Below the phone are icons for various platforms: Windows, iOS, Android, Android TV, Linux, Unity, and LG WebOS. The text "Supported platforms" is centered above these icons.

Figure 1: Advertising from PacketSDK, part of the IPIDEA proxy network

To learn more:

<https://cloud.google.com/blog/topics/threat-intelligence/disrupting-largest-residential-proxy-network>



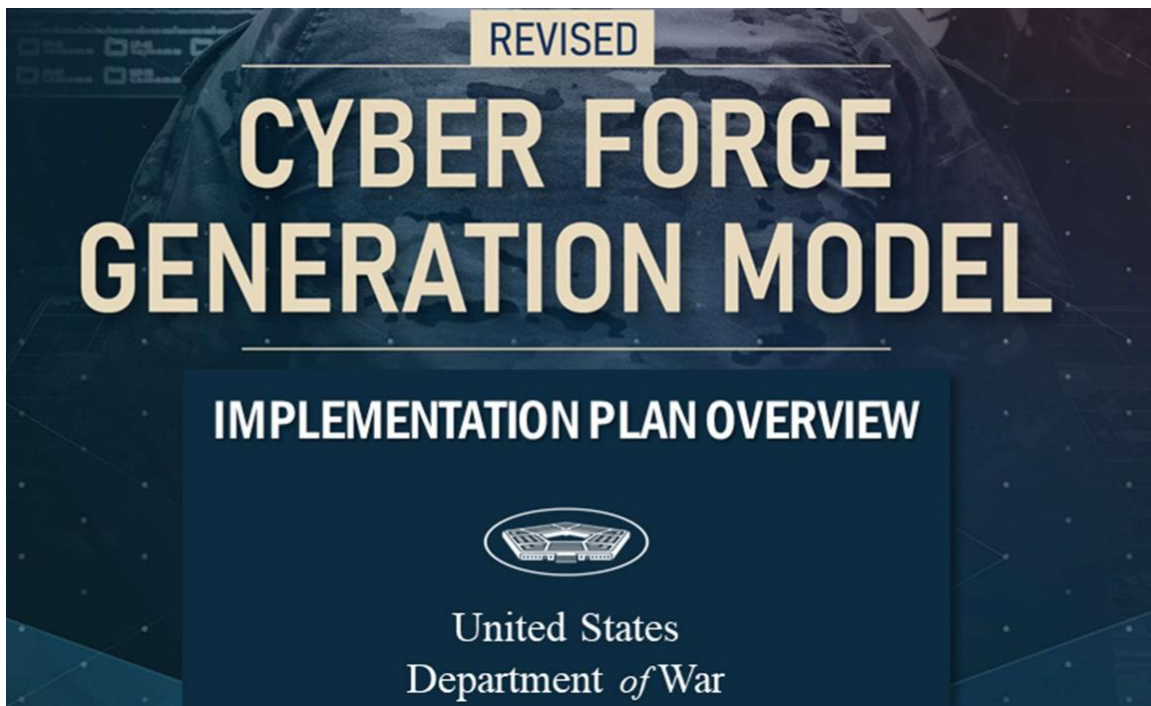
Number 10

Subcommittee on **Cybersecurity** - To receive testimony on the Department's cyber force generation plan and the associated implementation plan



The video:

<https://www.armed-services.senate.gov/hearings/to-receive-testimony-on-the-departments-cyber-force-generation-plan-and-the-associated-implementation-plan>



Pillar 1 - Domain Mastery: The DoW is fundamentally shifting away from a compliance-based training paradigm to one that fosters deep, career-long expertise. Our objective is to cultivate a cadre of cyber professionals who achieve true mastery in cyberspace, rather than rotating through cyber assignments as generalists. This approach builds a cyber force better capable of addressing emerging threats, such as adversaries exploiting industrial control systems in critical infrastructure or leveraging artificial intelligence to automate cyberattacks. CYBERCOM 2.0 enables increased influence by the Commander, USCYBERCOM in the talent management of the Department's cyber forces. For example, instead of cyber operators rotating out after a basic qualification, they will have a career path that allows for extended tours in the Cyber Mission Force (CMF), followed by an assignment with a Military Service (Service) cyber unit to broaden their experience and bring their deep expertise back to their Service formations. This model cultivates unrivaled experts who possess a deep portfolio of experience in specific, mission-critical areas.

Pillar 2 - Specialization: The cyber domain is incredibly diverse; as such, a traditional one-size-fits-all approach to force generation is ill-suited to deliver the operational outcomes required. CYBERCOM 2.0 establishes dedicated pathways for our cyber forces to develop deep expertise in highly specialized fields such as cloud security architecture, industrial control systems, and artificial intelligence. This will result in the formation of dedicated units of specialized experts aligned to critical missions, such as a team with expertise in space asset protection or another focused on securing critical energy infrastructure.

To learn more:

https://www.armed-services.senate.gov/imo/media/doc/cybercom_public_summary.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 prejudice 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 prejudice 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>

International Association of Risk and Compliance Professionals (IARCP)



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>

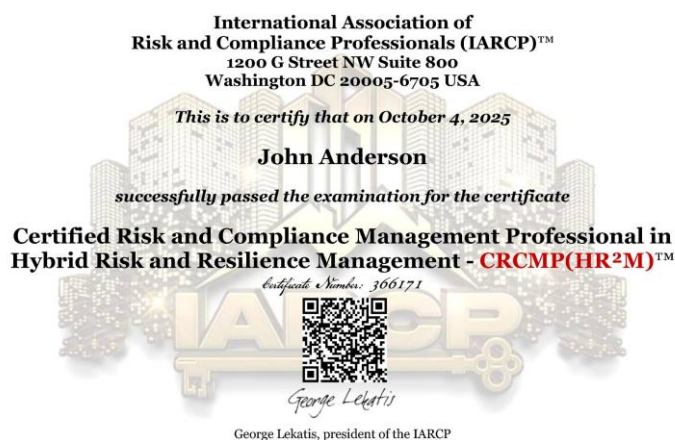
The CRCMP has become one of the most recognized certificates in risk management and compliance. There are CRCMPs in fifty-seven countries. Companies and organizations around the world consider the CRCMP a preferred certificate.

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](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](https://www.risk-compliance-association.com/TSecTPro_Distance_Learning_and_Certification.htm)

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

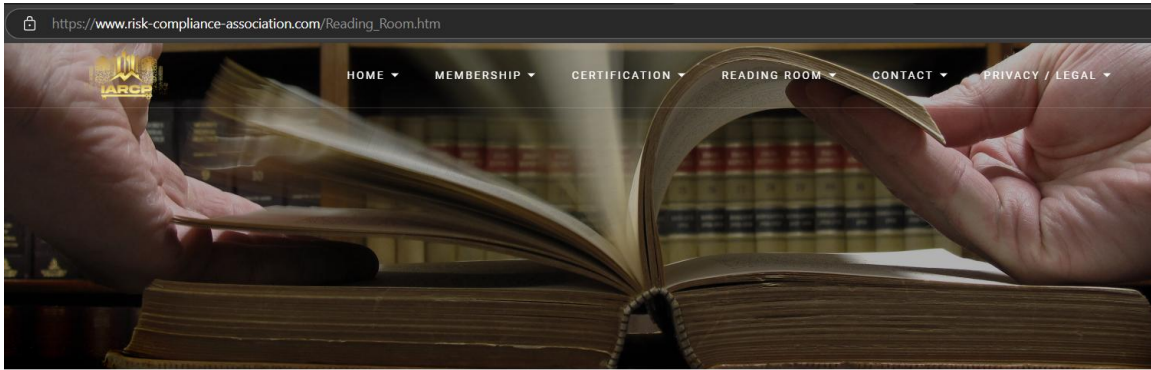
Overview

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

