Monday, December 15, 2025

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

New terms, and their definitions, are always interesting. Of course, we may end up with a phrase that ages as badly as *cyberspace superhighway*, but if it doesn't stick, we can always rebrand it as ahead of its time and, of course, visionary.

Christine Lagarde, speaking in Helsinki (at the Bank of Finland's 4th Monetary Policy Conference "Monetary policy in the shadow of geopolitical tensions and trade conflicts"), said:

"We find ourselves in a new world, one where policymakers can no longer confine themselves to traditional economic and financial variables. Now, we must factor "geoeconomics" into our analyses. The term was coined in 1990 by Edward Luttwak, who described geoeconomics as "the admixture of the logic of conflict with the methods of commerce".

I loved the word admixture in the description of what geoeconomics is. No, it is not mixture (anything made by combining two or more things). It is admixture, that implies a purposeful addition to something already existing.

Edward Luttwak coined the term geoeconomics in his 1990 essay *From Geopolitics to Geoeconomics: Logic of Conflict, Grammar of Commerce.*

His key insight was that countries compete for power and influence, and use military force and economic instruments (tariffs, export controls, sanctions, access to markets, control of technology, foreign investment, infrastructure finance).

Luttwak was saying that after the Cold War, military confrontation was less frequent, but states didn't stop competing, they simply shifted the battlefield to trade, finance, and technology, turning economics into a tool of strategy and conflict.

Take the logic of war. Apply it through the lens of economics (deals, investment, trade). The *admixture* is a statecraft using economic levers to weaken or outmaneuver rivals. And, as it is natural, nations compete with every tool they have.

The only strange thing is that economists, long busy fighting among themselves (free market vs. protectionism, liberalization vs. industrial policy) are now forced to watch the reality unfold. Theories about open competition and efficiency still run into a world where states use tariffs, export controls, supply chain controls and restrictions, and financial sanctions, as weapons. The polite seminar on trade theory has turned into a bootcamp with supply chains as hostages and economic models in warfare manuals.

In the old economics syllabus, we read supply and demand. In the new syllabus, we read supply, demand… and how to weaponize them.

The concept of comparative advantage was first formulated by the British economist David Ricardo in his 1817 book *On the Principles of Political Economy and Taxation*. Ricardo explained why nations benefit from trade even if one country is more efficient at producing all goods. Each should specialize in what it produces relatively more efficiently, and trade for the rest. This was built on Adam Smith's absolute advantage. Ricardo's insight (that even a less productive country can gain from trade) was interesting.

Now we need a Ricardo 2.0, with a geopolitics plug-in, that will explain something like … specialize, but stockpile chips, diversify suppliers, harden your networks, never forget that today's trusted trade partner could become your adversary, or a puppet of an adversary.

Ricardo 1.0 believed we must specialize, trade, and everyone benefits. According to Ricardo 2.0, economic interdependence can be weaponized. Specialize, but never depend. Comparative advantage still matters, but strategic autonomy replaces efficiency.

Ricardo 2.0 still values cooperation, but it embeds a security premium into economic models. It teaches that efficiency without resilience is fragility.

Ricardo 3.0 will develop the *Comparative Advantage in the Age of Artificial Superintelligence*. He will live in a world where superhuman AI systems, whether corporate, national, or extraterritorial, reshape the foundations of economic advantage. Comparative advantage is about who controls the cognitive infrastructure of the global economy.

We will have the rise of cognitive export controls, and new jokes. What do you call an AI that secretly crosses a border without a license? An algorithmic fugitive.

Best regards,

George Lekatis
President of the IARCP

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

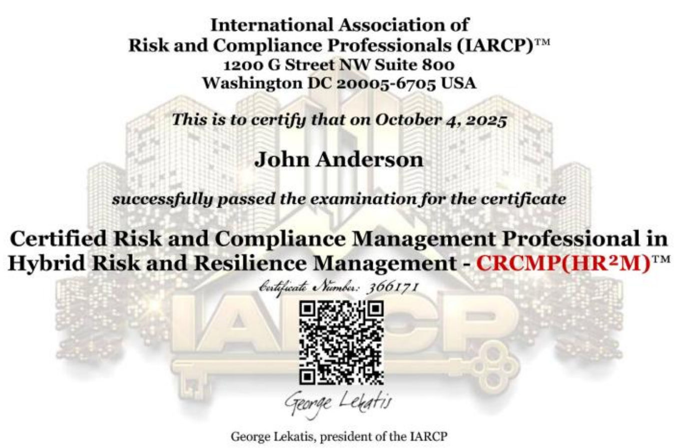
We are thrilled to announce the launch of the Certified Risk and Compliance Management Professional in Hybrid Risk and Resilience Management - CRCMP(HR²M), online training and certification program.

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


International Association of Risk and Compliance Professionals (IARCP)™
1200 G Street NW Suite 800
Washington DC 20005-6705 USA

This is to certify that on October 4, 2025

John Anderson

successfully passed the examination for the certificate

Certified Risk and Compliance Management Professional in Hybrid Risk and Resilience Management - CRCMP(HR²M)™

Certificate Number: 366171

George Lekatis

George Lekatis, president of the IARCP

Number 1 (Page 7)

Risk dashboard

Number 2 (Page 9)

Overview of planned consultation papers 2026

Number 3 (Page 11)

Supervision and Regulation Report

Number 4 (Page 13)

The rise of non-bank financial institutions: implications for monetary policy

Number 5 (Page 14)

Trade wars and central banks - lessons from 2025

Keynote speech by Ms Christine Lagarde, President of the European Central Bank, at the Bank of Finland's 4th Monetary Policy Conference "Monetary policy in the shadow of geopolitical tensions and trade conflicts", Helsinki.

Number 6 (Page 20)

Commission presents new Bioeconomy Strategy

European Commission

Number 7 (Page 23)

Spyware Allows Cyber Threat Actors to Target Users of Messaging Applications

Number 8 (Page 25)

Account Takeover Fraud via Impersonation of Financial Institution Support

Internet Crime Complaint Center (IC3)

Number 9 (Page 27)

Secure your mobile phone

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Number 10 (Page 29)

WHAT TO REPORT

Defense Counterintelligence and Security Agency

Number 1

Risk dashboard

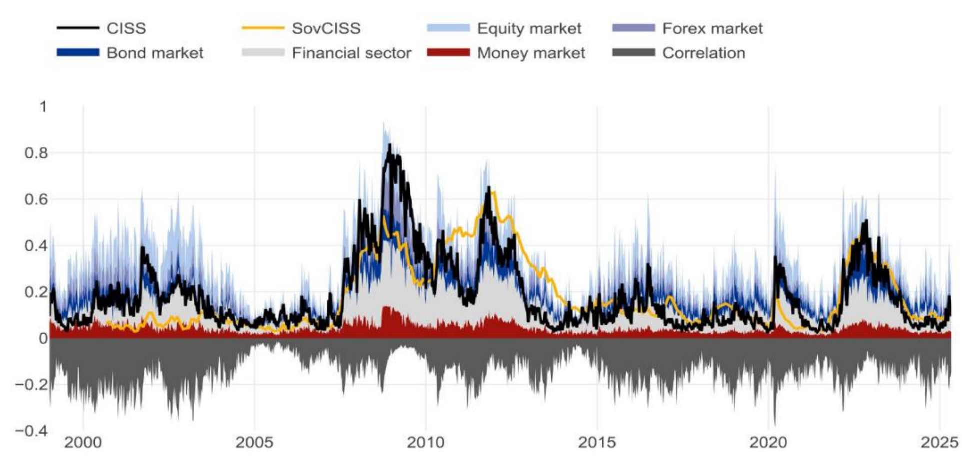
ESRB | EUROPEAN SYSTEMIC RISK BOARD

The ESRB risk dashboard is a set of quantitative and qualitative indicators of systemic risk in the EU financial system. It is published quarterly, one week after its adoption by the General Board, and is accompanied by two annexes that explain the methodology and describe the indicators.

The risk dashboard should not be considered to be a policy statement on systemic risks. Additional indicators that support systemic risk assessment in the EU financial system are available in the Macro-prudential database maintained by the ECB.

1.1 Composite indicator of systemic stress

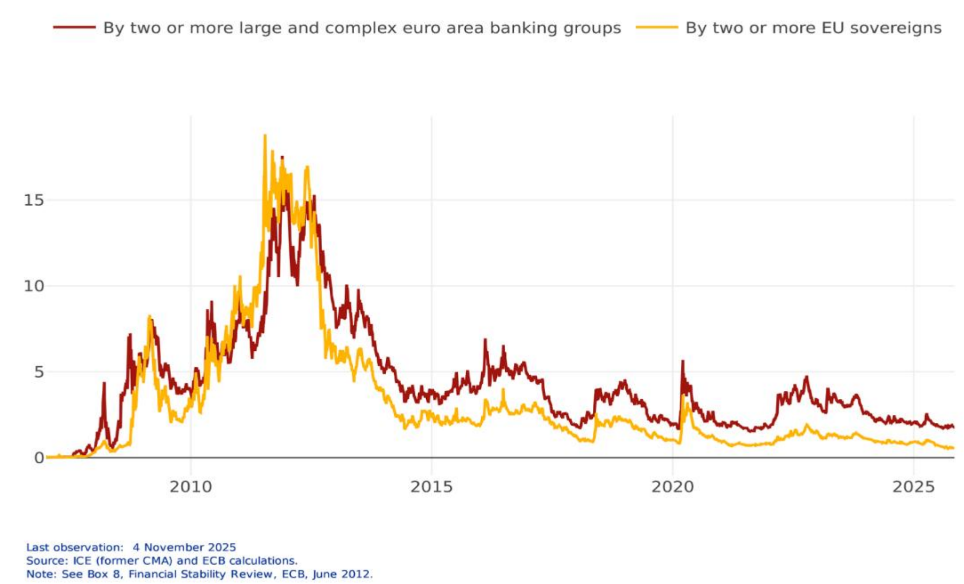
(Euro area; indicator)



Last observation: 2 May 2025
Source: LSEG, ECB and ECB calculations.
Note: The CISS is unit-free and constrained to lie within the interval (0, 1). See Hollo, D., Kremer, M. and Lo Duca, M., "CISS - a composite indicator of systemic stress in the financial system", Working Paper Series, No 1426, ECB, March 2012. The Sovereign CISS applies the same methodological concept of the CISS. On aggregation of different measures of stress in different euro area sovereign bond markets see Garcia-de-Andoain, C. and Kremer, M., "Beyond spreads: measuring sovereign market stress in the euro area", Economics Letters, Vol. 159, 2017, pp. 153-156.

1.2 Probability of a simultaneous default

(EU; probability of default; percentage points)



To learn more: https://www.esrb.europa.eu/pub/rd/html/index.en.html

https://www.esrb.europa.eu/pub/pdf/dashboard/esrb.risk_dashboard_external_251127~3b4a4e3c66.en.pdf?71d9e9d49debb3a1c1097b391c00fd80

Number 2

Overview of planned consultation papers 2026

The purpose of the table is to provide an overview of the planned consultations to help stakeholders in planning ahead. The table will be updated by ESMA on a regular basis. A list of ongoing and past consultations is available on ESMA's website.

Topic	Title of consultation paper	Planned publication of consultation paper
EMIR 3	RTS on post trade risk reduction services	Q1 2026
Listing Act	MAR Guidelines on Delay in the disclosure of inside information under the Listing Act	Q1 2026
EMIR 3	Update to RTS 153/2013 on guarantees	Q1 2026 (TBC)
CSDR Review	Guidelines on standardised procedures and messaging protocols (allocation and confirmation)	Q2 2026
CSDR Review	Guidelines on suitability of persons directing the business of a CSD and criteria for prudential assessment of acquisitions and increases of holdings in CSDs	Q2 2026
MiFIR	Extension of order book data-exchange mechanism between NCAs	Q2 2026
Investor Protection	Consultation paper on the revision of the MMF stress testing guidelines	Q2 2026
EMIR 3	Update to RTS 153/2013 collateral/investment	Q2 2026 (TBC)
Listing Act	Update to Guidelines on Prospectus Disclosure	Q3 2026
EMIR 3	Update to RTS 153/2013 on APC (TBC)	Q4 2026
Investor Protection	Retail Investment Strategy - Technical advice to the EC on investor protection topics (review of MiFID II Delegated acts)	H2 2026
Investor Protection	Retail Investment Strategy - Technical standards on investor protection topics	H2 2026
AIFMD/UCITS	AIFMD RTS on reporting	H2 2026
AIFMD/UCITS	UCITS RTS on reporting	H2 2026
AIFMD/UCITS	AIFMD ITS on reporting	H2 2026
AIFMD/UCITS	UCITS ITS on reporting	H2 2026

Other regulatory and supervisory priorities for 2026

Beyond the priorities coming from the SIU strategy, ESMA will continue supporting implementation of key legislative files agreed under the previous legislature, notably the European Market Infrastructure Regulation (EMIR 3) and the European Single Access Point (ESAP).

Other ongoing legislative files which, depending on progress, may require ESMA's attention in 2026 are the Retail Investment Strategy (RIS), as well as the review of the PRIIPS, SFDR and Securitisation Regulation. ESMA will ensure that it integrates the principles of Simplification and Burden Reduction across all its activities and will follow up on the 2025 'flagship' projects seeking simplification and efficiencies in disclosure and reporting frameworks.

Driving data innovation and market integration

ESMA will focus on enhancing data capabilities and promoting innovation across the EU financial sector. Key projects for 2026 include the rollout of the ESMA Data Platform, centralisation studies, and the development of AI-powered supervisory tools. These initiatives will bring common benefits to both ESMA and the National Competent Authorities, improving market efficiency and transparency through the support that data provides for risk-based and data-driven supervision across Europe.

In the digital finance sector ESMA will continue to focus on the effective implementation of MiCA, as it is key to ensuring investor protection and the orderly functioning of crypto-asset markets. ESMA's supervisory convergence efforts will remain focused notably on the authorisation and supervision of CASPs.

Finally, in line with the EU's ambition to accelerate the settlement cycle to T+1 by 11 October 2027, ESMA will also coordinate closely with market participants to ensure the smooth transition and preparedness of the financial sector for this event.

To learn more:
https://www.esma.europa.eu/sites/default/files/2025-11/ESMA22-50751485-1644_Stakeholders_forward_planning_table_2026.pdf

Number 3

Supervision and Regulation Report

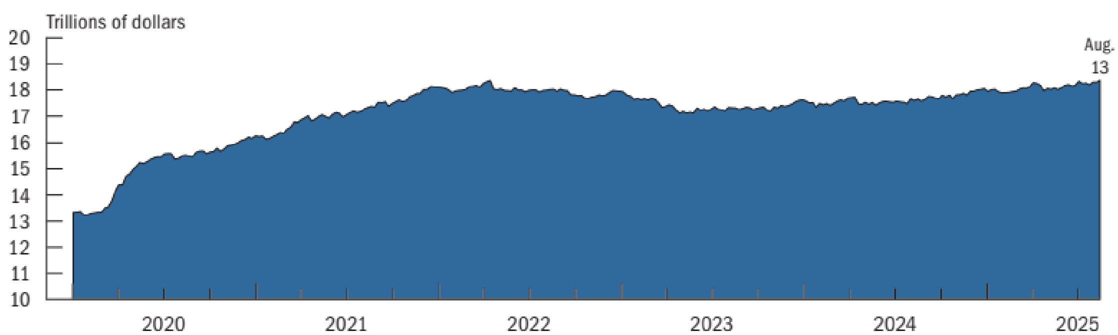
The Federal Reserve Board publishes its semiannual Supervision and Regulation Report to inform the public and provide transparency about its supervisory and regulatory policies and actions, as well as current banking conditions.

Previous reports are available at https://www.federalreserve.gov/publications/supervision-and-regulation-report.htm.

For more information on how the Federal Reserve promotes the safety and soundness of individual financial institutions and the financial system, see:
The Fed Explained: What the Central Bank Does at:
https://www.federalreserve.gov/aboutthefed/the-fed-explained.htm and visit the Supervision and Regulation webpage on the Board's public website at:
https://www.federalreserve.gov/supervisionreg.htm.

This report focuses on developments in three areas:
1. Banking System Conditions provides an overview of the financial condition of the banking sector.
2. Regulatory Developments outlines the Federal Reserve's recent regulatory policy work.
3. Supervisory Developments highlights the Federal Reserve's current supervisory programs and priorities.

Figure 3. Deposits



Note: Data are seasonally adjusted and for all commercial banks.

Source: H.8, "Assets and Liabilities of Commercial Banks in the United States."

Figure 15. Outstanding supervisory findings by category, CBO firms

Note: As of 2025:Q2, there were 1,359 total supervisory findings for CBO firms.

Source: Internal Federal Reserve supervisory databases.

To learn more:
https://www.federalreserve.gov/publications/files/202512-supervision-and-regulation-report.pdf

Number 4

The rise of non-bank financial institutions: implications for monetary policy

BIS

Key takeaways

• Non-bank financial institutions (NBFIs) have grown significantly in recent years, mainly driven by the growth of investment funds, including hedge funds. These changes reflect the role of bond markets, which have expanded on the back of surging government debt.

• The rise of NBFIs adds uncertainty to monetary policy transmission, as there could be dampening and amplifying effects. Investment funds appear to strengthen transmission while at the same time making it less stable.

• Greater uncertainty about transmission due to structural changes in the financial system reinforces the principle of a gradual policy approach while at the same time calling for flexibility in adjusting policy.

The Great Financial Crisis put in motion a major structural change in the global financial system, with nonbank financial institutions (NBFIs) assuming a greater role in financial intermediation. This Bulletin documents the rise of NBFIs over the past two decades, examines their influence on monetary policy transmission and discusses the implications for central banks.

To learn more: https://www.bis.org/publ/bisbull116.pdf

Number 5

Trade wars and central banks - lessons from 2025

Keynote speech by Ms Christine Lagarde, President of the European Central Bank, at the Bank of Finland's 4th Monetary Policy Conference "Monetary policy in the shadow of geopolitical tensions and trade conflicts", Helsinki.

Here in Finland, the idea that economics cannot be separated from geopolitics is hardly new. During the early 1990s, as the Soviet Union collapsed, Finland lost more than 10% of its GDP when trade with its eastern neighbour suddenly evaporated.

Few countries know better the costs of ignoring geopolitical realities.

Today, the rest of Europe is facing a similar reckoning. We find ourselves in a new world – one where policymakers can no longer confine themselves to traditional economic and financial variables. Now, we must factor "geoeconomics" into our analyses.

The term was coined in 1990 by Edward Luttwak, who described geoeconomics as "the admixture of the logic of conflict with the methods of commerce". It is not protectionism in the old sense of sheltering vulnerable industries. Instead, it is trade deployed as a tool of power, a strategy of influence and dominance.

This approach has been around for some time, most visibly during the US-China trade disputes that unfolded during the first Trump Administration. The unjustified war in Ukraine and the sanctions that followed have also reshaped the European landscape. But 2025 marks the first year in which Europe itself has been on the receiving end.

We currently face the highest tariffs since the days of Smoot-Hawley in the 1930s, imposed by our largest trading partner. Global trade is being reshaped as other countries respond to tariffs directed at them. And in the span of just a few months, we have seen a surge in trade uncertainty and sharp swings in exchange rates.

So now is a good time to take stock of what we have learned so far, and what this implies for monetary policy.

Trade wars: expectations versus reality

A year ago, most would have assumed that US tariffs rising from 1.5% to 13% would trigger a major adverse shock to the euro area economy. Indeed, most trade models judged the imposition of tariffs to be, on net, negative for euro area growth and likely positive for inflation, at least in the short run.

This was broadly our internal assessment in December of last year, albeit surrounded by considerable uncertainty. Three channels were usually seen as decisive in producing such an outcome.

First, retaliation. Reciprocal tariffs were expected to raise import costs and reverberate through supply chains. In most models, this retaliation channel was by far the largest driver of higher short-term inflation.

Second, the exchange rate. Tariffs were expected to trigger a depreciation of the euro against the dollar – driven by expectations of higher US rates and a smaller US trade deficit – thereby amplifying imported inflation.

Third, uncertainty. Elevated trade policy uncertainty was expected to weigh heavily on business investment and growth, often more than the direct effect of tariffs on exports themselves. This was expected to be the largest negative force on growth.

Yet some of these assumptions have not been borne out.

This is because the tariffs were not an isolated economic event, but a symptom of a broader geopolitical shift – one that triggered political economy dynamics beyond the reach of standard models.

Start with retaliation.

In Europe and globally, it has so far been limited. In response to the US tariffs on steel and aluminium, the EU announced counter-tariffs on around €26 billion worth of American goods, but suspended them once a deal was struck in July.

Pressure from major industrial groups to avoid a prolonged cycle of tit-for-tat measures, as well as concerns about jeopardising US support for the war in Ukraine, ultimately outweighed pure economic calculus.

As a result, we have not yet seen significant supply chain disruption. Global supply chain pressures remain contained, and in the euro area, bottleneck indicators are close to historical averages.

If anything, rather than blocked supply chains, the euro area is facing rising imports. The euro area's trade deficit with China has risen by around 10% this year, although this was driven more by weaker Chinese demand than by diverted trade flows.

The exchange rate has also not behaved as expected.

Rather than depreciating, the euro has appreciated substantially. Since the start of this year, it has risen by 13% against the US dollar, while the nominal effective exchange rate has increased by 6.5% and the real effective exchange rate by 5%.

This reflects the fact that the imposition of US tariffs coincided with a broader re-evaluation of the country's position in the global financial system.

Investors began to question whether the US dollar would continue to warrant its status as the ultimate safe-haven currency – another political-economy factor that narrow, tariff-focused models excluded by assumption.

The international role of the euro has helped insulate us from the resulting exchange rate volatility, with 52% of our imports invoiced in our own currency. But many key imports, especially commodities, are still priced in dollars.

The euro's appreciation has therefore contained imported inflation from supply chains, while at the same time placing an additional drag on growth.

The effects of uncertainty have been more in line with expectations. The expected cumulative impact of tariffs and uncertainty on growth is around 0.7 percentage points between 2025 and 2027, compared with our projections last December.

Still, these effects have not been as strong as we anticipated. For example, only about a quarter of the downward revision for next year, compared with December last year, is due to uncertainty.

This is partly because trade policy uncertainty fell faster than we expected once the deal with the United States was concluded. It is also because the euro area has taken internal measures to boost growth that have helped counter external weakness.

In particular, governments in Europe have committed to the largest increase in rearmament in decades, with some reversing years of underinvestment. Government investment is now expected to add 0.25 percentage points to growth between 2025 and 2027, offsetting around one-third of the trade shock.

The EU has also pushed ahead with new trade agreements, which will support growth. The Mercosur and Mexico deals now being adopted cover more than 3% of extra-euro area goods exports, while agreements currently under negotiation account for a further 6%.

This is another example of a response that models could not capture beforehand: trade pressures have led European governments to re-evaluate their broader trade and security relationships, prompting an endogenous investment response.

All in all, with no retaliation and an appreciating exchange rate, tariffs have had little inflationary impact so far, with their adverse effects mainly limited to growth. Those effects, however, have been relatively moderate thanks to the domestic response.

Evaluating the balance of risks

In an environment of high uncertainty, understanding the nature of shocks is a precondition for getting the baseline projection right.

But capturing the balance of risks is just as crucial, so that we are prepared for a situation in which the baseline may prove obsolete and can act pre-emptively, if necessary.

This was a key conclusion of our recent strategy review: to emphasise more risks and uncertainty in our decisions, not just central projections.

Initially, we viewed the risks to growth from US tariffs as tilted to the downside.

This assessment was informed by extensive scenario analysis, including escalation scenarios and possible offsetting forces – notably the growth impact of a sustained increase in defence and infrastructure spending.

Overall, these scenarios have consistently shown that the most salient risks – those that could push growth furthest from its current path – lie on the downside rather than the upside.

For example, ECB staff find that severe escalation in trade tensions could lower growth cumulatively by about 1 percentage point over the projection horizon.8 The potential boost from higher defence spending would not be sufficient to offset this, even if all countries were to deliver fully on their NATO commitments.

This tilt in the risk balance remains in place today. But at our last meeting, we judged risks to growth to be more balanced, because the likelihood of major tariff-related downside risks materialising had fallen owing to the new trade deal.

Meanwhile, we judged inflation risks to be two-sided, with plausible scenarios that could push inflation off track in either direction. But as new information has come in, the range of risks on both sides has also narrowed.

In particular, the absence of significant EU retaliation has reduced the risk that higher import tariffs might drive inflation above the baseline. Our scenario analysis also points to inflation risks that remain well contained.

If trade tensions were to reignite, staff project only moderately lower inflation in 2027, reflecting weaker growth. Higher spending on defence equipment, by contrast, would only modestly raise inflation, given its relatively small weight in the consumption basket.

Staff have also examined scenarios that would affect prices more directly: on the downside, Chinese export prices being lowered further as a strategic response to tariffs; and on the upside, more pronounced bottlenecks in global supply chains.

In both cases, however, the impact would be limited under reasonable assumptions, with inflation in 2027 differing by only 0.1-0.2 percentage points.

Policy implications

So what does this imply for our monetary policy?

I have said that we are in a good place. This was largely a reference to the fading of the large inflation shock we faced in recent years, which is now essentially over in the euro area.

But there are also three additional reasons why it applies to the current situation.

First, because trade shocks are not creating new inflationary pressures, we are not confronted with the classic policy trade-off where the central bank faces stalling growth and rising inflation.

This has already allowed us to cut policy rates by 100 basis points since December – cushioning the impact while keeping medium-term inflation on track.

Second, insofar as we can model the future, the risks to inflation appear quite contained in both directions.

Third, with policy rates now at 2%, we are well placed to respond if the risks to inflation shift, or if new shocks emerge that threaten our target.

At the same time, we are navigating a far more difficult environment than before – beset by war, tariffs and uncertainty – which we must also factor into our policy.

If we consider the "known knowns", the risks appear well bounded.

But there are also "known unknowns" – above all, how euro area companies will adapt to this new setting. Firms are still running down inventories and absorbing the shock in margins, so the full effects of US tariffs have yet to become clear.10

Finally, there are the "unknown unknowns": in a world of geoeconomics, new trade and geopolitical shocks will remain a constant feature of our environment.

How these forces play out will have unavoidable effects on monetary policy – not only through their impact on growth, but also on potential growth.

If firms interpret the new environment as a lasting confidence shock, we could see investment shift out of the euro area. Preliminary staff analysis suggests that, all else being equal, tariffs are likely to weigh negatively on potential growth.

Lower potential growth would, in turn, put downward pressure on real rates and reduce the policy space available.

But other paths are possible if governments act decisively and give firms new reasons to be confident.

One factor often overlooked in the tariff debate is that our internal market is far more important for trade than the global market. Staff analysis shows that an increase of just 2% in intra-euro area trade would be enough to offset the loss of exports to the United States caused by higher tariffs.

This is a compelling reason to implement the reforms identified in recent reports from Mario Draghi and Enrico Letta, in particular simplifying burdensome regulation, completing the Single Market and building a genuine European capital market.

The same reforms would also help European companies adopt artificial intelligence more rapidly. This would result in a positive shock for potential growth, helping to balance the negative forces coming from abroad.

In short, nothing about our future is fate – and there is no room for complacency by any party.

For our part, we cannot pre-commit to any future rate path, whether one of action or inaction. We must remain agile, and ready to respond to the data as they come in.

Conclusion

Let me conclude.

This is an unusual time to be a monetary policymaker.

We can take comfort in having overcome a large inflation shock after the pandemic, and in how the economy has coped so far with an upheaval in trade relations.

And yet, we must remain alert to the possibility that not all the consequences are visible today – and that new shocks may still lie ahead.

As we look to the future, we do so mindful of Finland's long tradition of sisu – courage and inner strength in the face of uncertainty.

Sisu is not a show of fleeting bravery, but rather a fierce determination and perseverance to continue fighting even when times get tough.

We are in a good place today, but that place is not fixed. Our task is to sustain it with agility, humility and a firm grounding in the data.

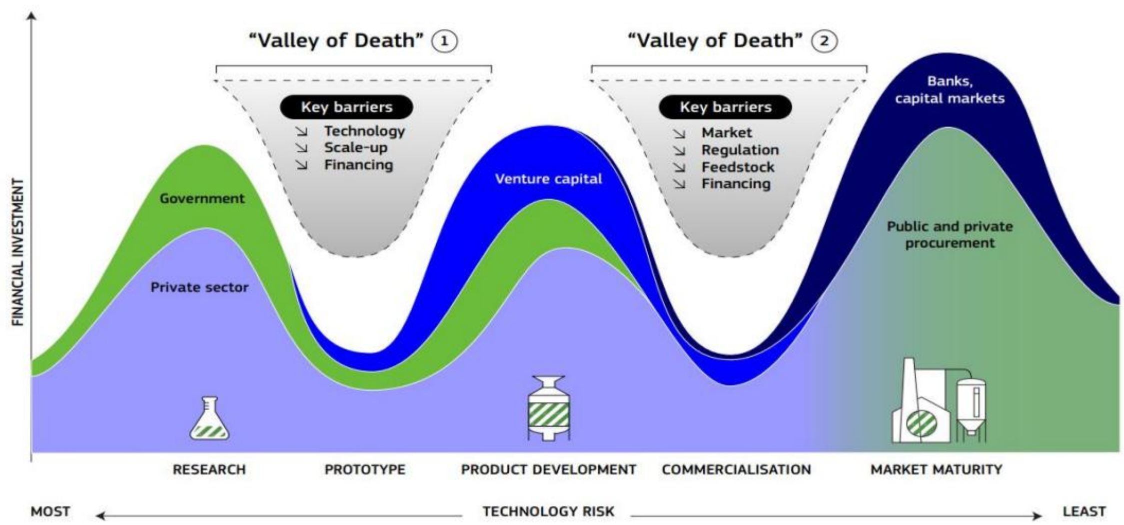
To learn more:
https://www.ecb.europa.eu/press/key/date/2025/html/ecb.sp250930~c973459788.en.html

Number 6

Commission presents new Bioeconomy Strategy

The Commission adopted a new Strategic Framework for a Competitive and Sustainable EU Bioeconomy, charting a way forward to build a clean, competitive and resilient European economy. By using renewable biological resources from land and sea and providing alternatives to critical raw materials, the EU will move forward towards a more circular and decarbonised economy and can decrease dependence on fossil imports.

Figure 2: Two valleys of death in scaling bioeconomy in Europe



Source: European Commission graph based on the public consultation results and own analysis

The bioeconomy offers Europe a chance to strengthen its resilience, replace fossil-based materials and products, create jobs and lead the global shift to clean industries.

With this new Strategy, the EU will support activities that provide sustainable practical solutions using our biological resources in sectors such as agriculture, forestry, fisheries, aquaculture, biomass processing, biomanufacturing and biotechnologies. It will harness the vast potential of these resources, scientific excellence and industrial base, and encourages innovations that benefit the climate, nature and society.

With a value of up to €2.7 trillion in 2023 and employing 17.1 million people (around 8% of EU jobs), the EU bioeconomy already contributes significantly to job creation and economic growth in Europe. Every job in the bioeconomy creates three indirect jobs in the EU.

Examples of products are bio-based chemicals made from algae that are used to produce pharmaceuticals, personal care products and industrial applications. Bio-based plastics are increasingly used in packaging and automotive parts.

Also, bio-based construction productions, textile fibres and fertilisers are increasingly in demand. However, it still has a huge untapped potential.

The EU Bioeconomy Strategy aims to unlock this potential by scaling up innovation and investments, developing lead markets for bio-based materials and technologies, ensuring a sustainable supply of biomass, and harnessing global opportunities.

ANNEX: Key Actions and Timeline

SCALING UP INNOVATION AND INVESTMENTS: FROM LAB TO DEPLOYMENT

Actions	Timeline
Adopt Biotech Acts	2025 3Q 2026
Establish a European Bioeconomy Regulators and Innovators' Forum	1Q2026
Adopt standardisation requests for doors & windows, structural timber products/elements and ancillaries, wood-based panels and elements, thermal insulation products under the Construction Products Regulation	2026
Support co-operation of primary producers to drive joint investments in innovative bio-based value chains through CAP investment support, sectoral interventions and the European Innovation Partnership	2026
Launch of a European Bioeconomy Investment Deployment Group	2026-2028

INTRODUCTION

The bioeconomy represents a strategic opportunity of the 21st century - a driver of green growth, competitiveness and resilience. It makes better use of Europe's biological resources, scientific excellence and industrial base to decarbonise our economy and replace fossil-based materials and products. It develops practical solutions that support economic prosperity, and strong rural and coastal communities, while helping industry shift to more circular production models. It contributes to the EU's strategic autonomy by reducing reliance on imported fossil-based products and can contribute significantly to climate and environmental goals such as resource efficiency, greenhouse gas emissions reduction, water resilience, zero pollution and biodiversity.

The bioeconomy is defined as the activities that deliver sustainable solutions based on **biological resources to create added value**. These include products, services, science and technologies benefiting sectors ranging from agriculture, forestry, fisheries and aquaculture to value chains based on biomass processing, biomanufacturing and biotechnologies such as in food[1], health, energy, industry, ecosystem and other services. Biological resources[2] include genetic resources, as well as primary and secondary biomass, such as by-products and residues, and biogenic carbon[3] captured through innovative technologies.

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

A Strategic Framework for a Competitive and Sustainable EU Bioeconomy

{SWD(2025) 895 final}

To learn more:
https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2819

https://environment.ec.europa.eu/document/download/dbf8d2ba-9332-4f7a-b336-f356fa4b7236_en?filename=COM_2025_960_1_EN_ACT_part1_v10_0.pdf

Number 7

Spyware Allows Cyber Threat Actors to Target Users of Messaging Applications

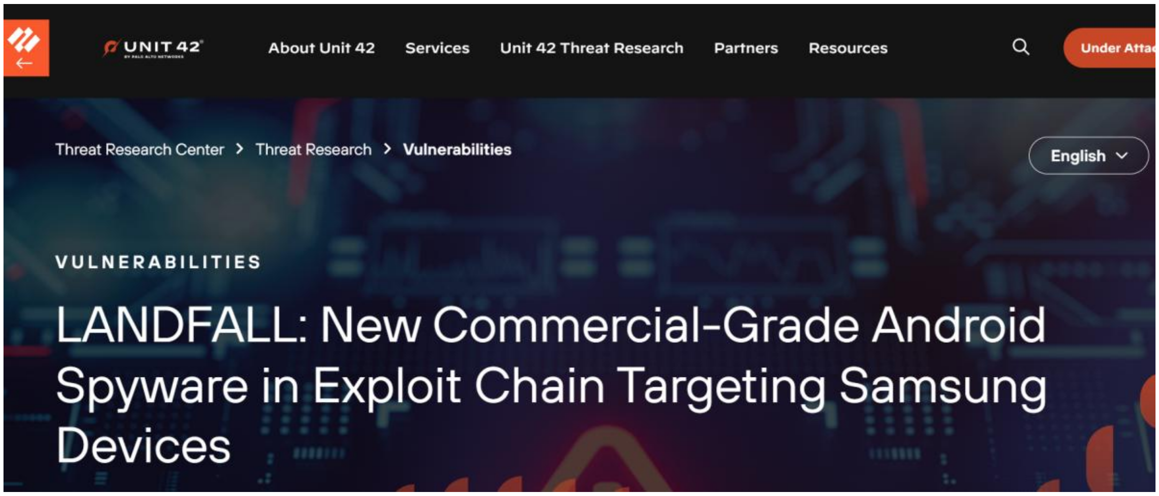
CISA is aware of multiple cyber threat actors actively leveraging commercial spyware to target users of mobile messaging applications (apps). These cyber actors use sophisticated targeting and social engineering techniques to deliver spyware and gain unauthorized access to a victim's messaging app, facilitating the deployment of additional malicious payloads that can further compromise the victim's mobile device.

These cyber actors use tactics such as:

- Phishing and malicious device-linking QR codes to compromise victim accounts and link them to actor-controlled devices.
- Zero-click exploits, which require no direct action from the device user.
- Impersonation of messaging app platforms, such as Signal and WhatsApp.

While current targeting remains opportunistic, evidence suggests these cyber actors focus on high-value individuals, such as current and former high-ranking government, military, and political officials, as well as civil society organizations (CSOs) and individuals across the United States, Middle East, and Europe.

CISA strongly encourages messaging app users to review the updated Mobile Communications Best Practice Guidance and Mitigating Cyber Threats with Limited Resources: Guidance for Civil Society for steps to protect mobile communications and messaging apps, as well as mitigations against spyware.



To learn more:
https://www.cisa.gov/news-events/alerts/2025/11/24/spyware-allows-cyber-threat-actors-target-users-messaging-applications

Number 8

Account Takeover Fraud via Impersonation of Financial Institution Support

The FBI warns of cyber criminals impersonating financial institutions to steal money or information in Account Takeover (ATO) fraud schemes. The cyber criminals target individuals, businesses, and organizations of varied sizes and across sectors.

In ATO fraud, cyber criminals gain unauthorized access to the targeted online financial institution, payroll, or health savings account, with the goal of stealing money or information for personal gain. Since January 2025, the FBI Internet Crime Complaint Center (IC3) received more than 5,100 complaints reporting ATO fraud, with losses exceeding $262 million.

How It Works

The cyber criminal impersonates the financial institution's staff or website, to obtain access to the account. Cyber criminals usually gain access to accounts through social engineering techniques — including texts, calls, and emails — or through fraudulent websites.

Social Engineering

- A cyber criminal manipulates the account owner into giving away their login credentials, including multi-factor authentication (MFA) code or One-Time Passcode (OTP), by impersonating a financial institution employee, customer support, or technical support personnel. The cyber criminal then uses login credentials to log into the legitimate financial institution website and initiate a password reset, ultimately gaining full control of the accounts.

- Social engineering methods include contacting account owners via fraudulent text messages, calls, or emails to trick the email recipient into providing their login credentials. In some instances, the cyber criminal states there are fraudulent transactions on the financial account and may provide a link to a phishing website that the account owner believes will report the fraud or prevent additional fraudulent transactions.

- In some instances, cyber criminals impersonating financial institutions reported to the account owner that their information was used to make fraudulent purchases, including firearms. The cyber criminal convinces the account owner to provide information to a second cyber criminal impersonating law enforcement, who then convinces the account owner to provide account information.

Phishing Domains/Websites

- The cyber criminal uses a phishing website that looks like the legitimate online financial institution or payroll website to trick the account owner into giving away their login credentials. Believing the phishing website is the legitimate one, users enter their login credentials into the fraudulent site, unknowingly providing them to cyber criminals.

- Cyber criminals may also use a technique called Search Engine Optimization (SEO) poisoning. SEO poisoning refers to cyber criminals purchasing ads that imitate legitimate business ads to increase the prominence of their phishing websites by making them appear more authentic to customers who use a search engine to locate the business' website. When users click on the fraudulent search engine ad, they are directed to a sophisticated fraudulent phishing site that mimics the real website, tricking users into providing their login information.

Once the impersonators have access and control of the accounts, the cyber criminals quickly wire funds to other criminal-controlled accounts, many of which are linked to cryptocurrency wallets; therefore, funds are disbursed quickly and are difficult to trace and recover. In some cases, including nearly all social engineering cases, the cyber criminals change the online account password, locking the owner out of their own financial account(s).

To learn more: https://www.ic3.gov/PSA/2025/PSA251125

Number 9

Secure your mobile phone

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Protect your phone or tablet from cybercriminals.

If your phone is lost or compromised, your information could be at risk. Protecting your mobile phone is just as important as protecting your computer or your wallet. If someone gets access to your phone, they could also get easy access to:

- your email and social media accounts
- your messages and contacts
- your photos, videos and notes
- your banking or financial details
- any apps you use and the data you store in them
- your browser history.

Follow these steps to secure your phone and protect your information. Most of these steps are free and easy to do and can also be used to secure your tablet.

Keep your phone locked and physically secure

- Lock your phone with a passphrase, password, PIN or biometrics. Make it difficult to guess – simple patterns or your date of birth are too easy. You should consider using facial recognition or a fingerprint to unlock your device if it has this option. This way, people can't watch what you use for your password or PIN.

- Ensure your phone is set to automatically lock after a short time of inactivity, such as five minutes. The shorter the better.

- Treat your phone like your wallet. Keep it safe or with you at all times.

- Encrypt the data on your phone. Even though your phone might be locked, someone could still access your phone's onboard data storage and information if it is not encrypted. Recent versions of Apple iOS or Google Android now also have encryption options available. Encryption of some form has been included in mobile devices from iOS 3.0 and Android 4.0, and most devices will now ship with encryption turned on by default. This uses your normal PIN or screen lock passphrase/ password to protect your data.

- Use your phone's remote tracking features (such as Apple's Find my iPhone or Google's Find your phone) to help find your phone or remotely erase the contents if it is lost or stolen.

Regularly back up your phone

- Backing up the data on your phone is important and should be done regularly. This will help you recover your data if your phone is ever lost, stolen or damaged. Backups of important information should be kept on at least two other devices. For more information, read our advice for backups.

Update your phone's software

- Turn on automatic updates for your phone's operating system and apps to install new updates as soon as they are available. This is often done through your phone's settings menu. Updates help to correct security vulnerabilities that could be used by cybercriminals to access your phone or information. Your phone may need to be connected to Wi-Fi and a charger to install the updates. If you need help, the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) has published guidance on how to update your phone.

Be careful using free or public Wi-Fi

- Public Wi-Fi 'hotspots' like cafes, airports, hotels and libraries are convenient, but they can be risky. It's easy for information sent using public Wi-Fi to be intercepted, so you should be careful about what information you send or receive while connected. Ideally, use **cellular data** when not connected to your own Wi-Fi network.
- **Do not let your device automatically connect to public Wi-Fi networks**. You can turn this off in your phone's Wi-Fi settings.

To learn more:
https://www.cyber.gov.au/protect-yourself/securing-your-devices/how-secure-your-devices/secure-your-mobile-phone?utm_source=x&utm_campaign=jul-25&utm_medium=social&utm_content=secure-your-mobile

Number 10

WHAT TO REPORT

Defense Counterintelligence
and Security Agency

WHAT TO REPORT

• All cyberthreats

• Aggressive port scanning outside normal network noise

• Advanced techniques / evasion techniques

• Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading

• Social engineering, electronic elicitation, email spoofing, spear phishing, whale phishing, or direct questioning

• Unauthorized network access

• Actual or attempted unauthorized access into U.S. information systems

• Tampering with or introducing unauthorized elements into information systems

•Unexplained storage of encrypted data

• Unexplained user accounts, administrator accounts, and expansion of network privileges

• Data exfiltration

• Malicious codes or blended threats

• Unauthorized email traffic to foreign destinations

• Use of Department of Defense (DoD) account credentials by unauthorized parties

• Network spillage incidents or information compromise

• Unauthorized transmissions of classified or CUI

• Any cyberactivity linked to suspicious indicators provided by DCSA, or by any other cyber centers and government agencies

HOW ARE YOU VULNERABLE?

- Publicly available information
- Contract information
- Company websites with technical/program data
- Connections (partnerships, key suppliers, joint ventures, etc.) with other cleared or uncleared companies
- Employee association with companies or technologies made public through scientific journals, academia, social networking sites such as Facebook and LinkedIn, etc.

PERSISTENT AND EMERGING CYBER THREATS

- Deepfakes: Creating fake images, sounds, and videos to fool the viewer
- Poisoning Attacks: Malicious injection into artificial intelligence program while it is learning
- Ransomware: New tactics, techniques, and procedures to exfiltrate data and release to the public
- Supply chain vulnerabilities
- Unsecure security products
- Malicious code injection
- Botnets
- Brute force
- Social network sites
- Credential harvesting

To learn more:
https://www.dcsa.mil/Portals/128/Documents/CI/DCSA%20Outreach%20Pamphlet_Cyber%20Threats_2024.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.

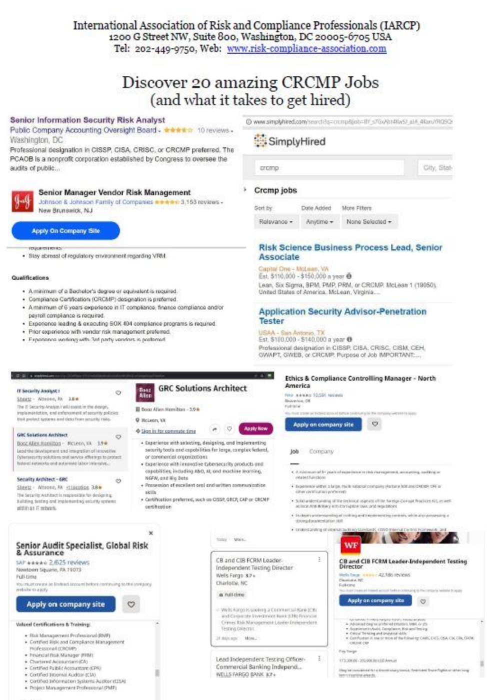
To learn more: https://www.risk-compliance-association.com/Privacy.htm

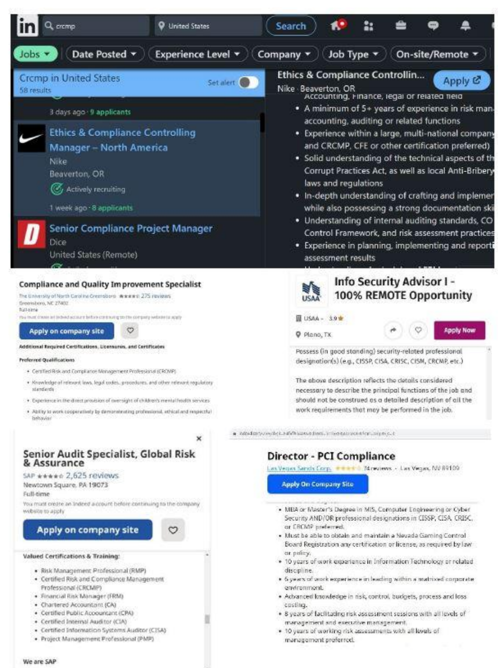
Our training and certification programs:

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(HR^{2}M), online training and certification program. You may visit: https://www.risk-compliance-association.com/CRCMP_HR2M.htm

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

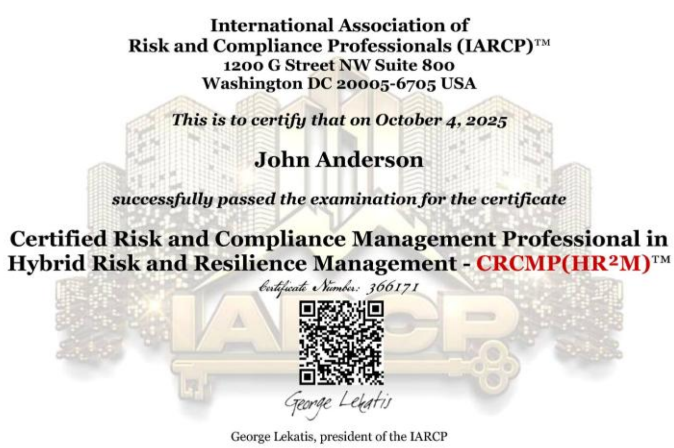
1. Moves from traditional risk and compliance frameworks into the management of multi-vector, cross-domain, and asymmetric threats that transcend conventional boundaries.

2. Develops expertise in hybrid risk governance.

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

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

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



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

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

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

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

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

Overview

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

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

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

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

Overview

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

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

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

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

Overview

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

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

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

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

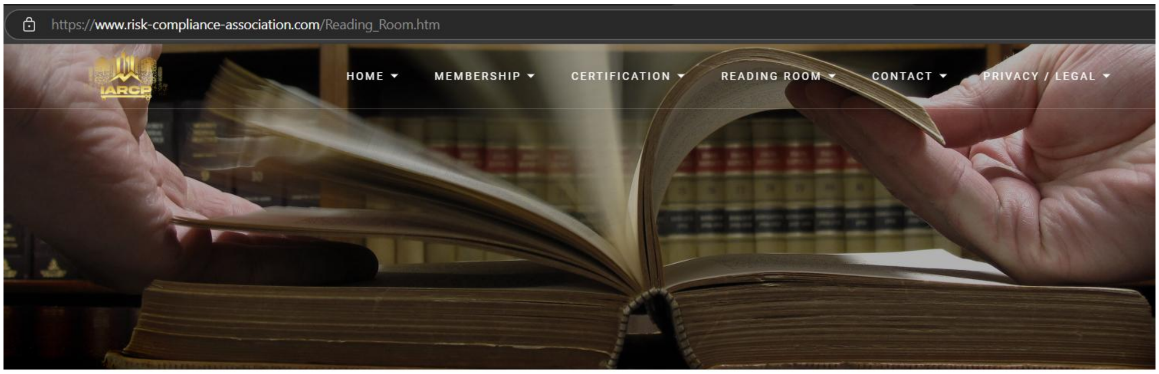
Overview

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

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

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

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



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

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

You may contact:

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

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