Monday, November 10, 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.

This 61-page argument was great, proving that bank supervision is an empirical science, a practiced art, and sustained almost entirely by caffeine. It was about *lessons on supervisory effectiveness, a literature review,* from the BIS.

The phrase early warning appears 35 times in 61 pages. We read:

"Early warning tools (e.g. indicators, models or systems) provide supervisors with insights about the health of a financial institution. Some studies indicate that technological advances in recent years, for example the use of machine learning, have improved the predictive power of the tools. It has been argued that an expanded use of market data in bank supervision is valuable because it complements information gathered by examiners, even if market signals are not superior to supervisory assessments. The model outcomes can provide a "second opinion" and also support decision-making on priorities. Important aspects for their use in practice are explainability, complementing quantitative results with qualitative insights and ensuring trust in the approach, for example by allowing for thorough testing."

This is an approach I truly valued, clear, balanced, and well-rounded. This second opinion is like asking Dr. Google after you've already seen the doctor. But what is an "early warning?"

Laws and regulations normally treat the term early in its ordinary English sense, *before the usual or required time, or in advance of a deadline or expected event*. Courts and statutes rely on the ordinary meaning, unless a special definition is given (see NIS 2 below).

What about the term early warning? This is a formal notification to identify and communicate the existence or likelihood of a risk, breach, or adverse event, so that competent authorities or obligated parties can take preventive or mitigating action before the situation escalates.

For example, in Article 23(4)(a) of the NIS 2 Directive of the EU (Directive 2022/2555), we read: "Without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning shall be submitted. The early warning shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact."

But what is an early warning tool? It is any technological or procedural mechanism, recognised by law or regulation, that detects and signals potential risks, breaches, or vulnerabilities at an initial stage, enabling to act before the threat or adverse event materialises.

Early warning in insider threat, is the detection and timely flagging of behavioral, digital, or organizational indicators suggesting that a trusted individual may intentionally or unintentionally pose a security risk. In psychology, early warning is the identification and monitoring of initial signs of psychological distress, disorder recurrence, or crisis risk, enabling timely preventive or therapeutic action.

I had to give a presentation explaining early warning, related to the NIS 2 implementation, to and IT team. IT experts often dislike me on sight. Then I say, *I still code in assembly,* and, of course, give an example and answer a question. I tell them that I still play with the Zero and Carry Flags, and a single wrong check transforms elegant code into an infinite loop or a crash. At this point I'm invited to the secret club. (Most of them still look at me like I'm a rare Pokémon).

I remember how I started:

There are three colleagues who meet every morning at the office coffee machine. They are called Early, Early Warning, and Early Earning Tool.

Early is the one who shows up before everyone else. She's there when the lights are still off and the cleaning crew is finishing. She doesn't predict the future, she's just ahead of schedule. In law and business, early usually means just that, before the usual or required time. No magic, only punctuality.

Then comes Early Warning, slightly dramatic but lifesaving. He doesn't just arrive early. He shouts: "Hey! The server's acting weird!" In legal and regulatory language, Early Warning is the formal alert or signal. Like a cyber-incident notice. Its purpose is to tell the bad news early enough to fix it.

Finally, the Early Earning Tool comes, sipping a latte. She's about making money before the rest of the office wakes up, turning foresight into profit.

Regulators ask for the second one. Your CFO hates the last one. And all three share one universal fuel, coffee.

Article 23 of NIS 2 speaks about the second colleague only, Early Warning. "Hey, within 24 hours of becoming aware of a significant incident, you must warn the national CSIRT or competent authority. Send Early Warning to explain whether the significant incident is suspected of being caused by unlawful or malicious acts, or could have a cross-border impact." It's not supposed to be a 200-page forensic report. It is more like: "Something bad is happening, here's what we know so far: yes/no it's malicious, yes/no it might spill into other countries, we're still figuring out the details."

This isn't panic, this is pre-panic. That's why we call it early warning.

Best regards,

George Lekatis
President of the IARCP

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

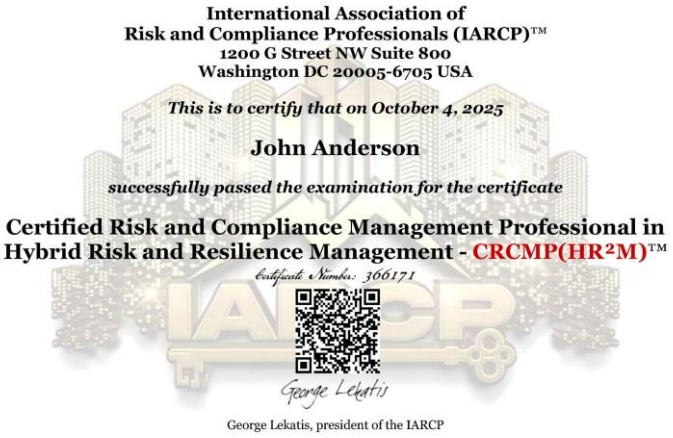
We are thrilled to announce the launch of the Certified Risk and Compliance Management Professional in Hybrid Risk and Resilience Management - CRCMP(HR²M), online training and certification program.

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

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

Enrollment in the CRCMP(HR²M) program is restricted to professionals who have already passed the CRCMP exam. To preserve the credibility and value of this credential, the association does not allow substitutions, equivalency credits, or waivers of any kind. The curriculum assumes mastery of the CRCMP body of knowledge.

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



Number 1 (Page 7)

Commission work programme 2026

Number 2 (Page 10)

Basel III monitoring report, October 2025

Number 3 (Page 13)

Vigilance Across Borders: The Global Imperative for Audit Quality
George R. Botic, Acting Chair, at the 17th Annual PCAOB International Institute Washington, DC

Number 4 (Page 19)

Opening Remarks
Michelle W. Bowman, Vice Chair for Supervision of the Board of Governors of the Federal Reserve System, at the Economic Growth and Regulatory Paperwork Reduction Act Outreach Meeting, Federal Reserve Bank of Kansas City, Kansas City, Missouri

Number 5 (Page 23)

Commission preliminarily finds TikTok and Meta in breach of their transparency obligations under the Digital Services Act

European Commission

Number 6 (Page 26)

The EBA consults on revised Guidelines on supervisory review and evaluation process and supervisory stress testing

eba European Banking Authority

Number 7 (Page 29)

Eurosystem moving to next phase of digital euro project

EUROPEAN CENTRAL BANK
EUROSYSTEM

Number 8 (Page 33)

The transformation of the life insurance industry: systemic risks and policy challenges

BIS

Number 9 (Page 35)

Don't take BADCANDY from strangers – How your devices could be implanted and what to do about it

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Number 10 (Page 37)

Dissecting YouTube's Malware Distribution Network

cp<r> CHECK POINT RESEARCH BY CHECK POINT

Number 1

Commission work programme 2026

EUROPEAN COMMISSION

Since this Commission took office, Europe has had to confront a world in its most precarious state for decades. From threats to our security and democracy to risks to our economy and industry, including the reckless airspace incursions and attempts at economic coercions we have witnessed in the past months, and Russia's ongoing war of aggression against Ukraine.

These challenges have come at a time when the international order – on which Europe's security and prosperity has long relied – is rapidly fraying. Against this backdrop, this must be Europe's Independence Moment. Europe must step up to secure and shape its own future.

28th Regime for Innovative Companies	(legislative, Articles 50 and 114 TFEU, Q1 2026)
European Innovation Act	(legislative, Articles 114, 173 and 182 TFEU, Q1 2026)
Public Procurement Act	(legislative, Article 114 TFEU, Q2 2026)
Advanced Materials Act	(legislative, Articles 114 and 173 TFEU, Q4 2026)
Cloud and AI Development Act	(legislative, Article 114 TFEU) and Chips Act (legislative, Articles 114 and 173 TFEU) (Q1 2026)
Critical Raw Materials Centre	(legislative, Article 114 TFEU, Q2 2026)
European Research Area Act	(legislative, Article 182 TFEU, Q3 2026)
European Biotech Act II	(legislative, Article 114 TFEU, Q3 2026)
Quantum Act	(legislative, Articles 173, 180 and 184 TFEU, Q2 2026)
Circular Economy Act	(legislative, Article 114 TFEU, Q3 2026)
European Product Act	
• Update of the new legislative framework of product rules	(legislative, Article 114 TFEU, Q3 2026)
• Update of rules on the market surveillance and compliance of products	(legislative, Articles 33 and 114 TFEU, Q3 2026)
• Update of rules on standardisation	(legislative, Article 114 TFEU, Q3 2026)
EU Delivery Act - update of rules on postal services	(legislative, Article 114 TFEU, Q3 2026)
Electrification action plan, including heating and cooling	(non-legislative, Q1 2026)
Strengthening Energy Security	(legislative, Article 194 TFEU, Q1 2026)
Update of the governance of the Energy Union and Climate Action including the phase-out of fossil fuels subsidies	(legislative, Articles 192 and 194 TFEU, Q4 2026)
Energy Union package for the decade ahead	
• Development of the CO_2 transportation infrastructure and markets	(legislative, Article 194 TFEU, Q3 2026)
• Setting-up of the energy efficiency framework	(legislative, Article 194 TFEU, Q3 2026)
• Setting-up of the renewable energy framework	(legislative, Article 194 TFEU, Q3 2026)
Omnibus to simplify energy product legislation	(legislative, Articles 192 and 194 TFEU, Q2 2026)

To protect its citizens from the impacts of climate change and reduce our impact on ecosystems. To be able to take care of its own defence and security. To take control over the technologies and energy sources that will power our economies.

To decide what kind of society and democracy we want to live in. To create quality jobs in a modern economy and strengthen our social model under changing demographic conditions. To develop the future of our European industry and support startups, scaleups and small businesses to thrive in our Single Market.

We will also focus on **unleashing the full potential of the Single Market by 2028** – removing barriers in capital, energy, services and telecoms, and enabling **a "fifth freedom"** for knowledge and innovation through the European Research Area. We will make doing business and accessing finance in Europe easier for all companies, not least innovative companies, startups and SMEs. We will establish a **European Innovation Act** and set up the **28th regime** for all companies operating across the Single Market, as well as putting forward the remaining proposals to complete the **Savings and Investment Union**. This will include the **strengthening of shareholder rights** and a comprehensive analysis on competitiveness in our banking sector. Moreover, with the **Cloud and AI Development Act** and the **Quantum Act** we will strengthen our digital sovereignty. And with the **Advanced Materials Act** we will support the technological leadership of our industry and European strategic autonomy.

To maintain our social, digital and environmental standards. To ensure that farmers receive a fair price for producing high quality food and to protect them from unfair trading practices. To be open to the world and choose partnerships with allies – old and new.

Ultimately, this is about having the freedom and the power to determine our own destiny. To deliver on this, Europe must stand united. It must draw on its collective strength and rally around the things we have in common. It must act with speed and a mindset of urgency to respond to the acute and unique requirements of the moment.

It needs boldness and ambition to match the scale of the challenges. It needs to focus on what matters the most to Europeans – from the cost of living to tackling illegal migration to protecting the environment – and simplify the way our laws work for people, communities and companies.

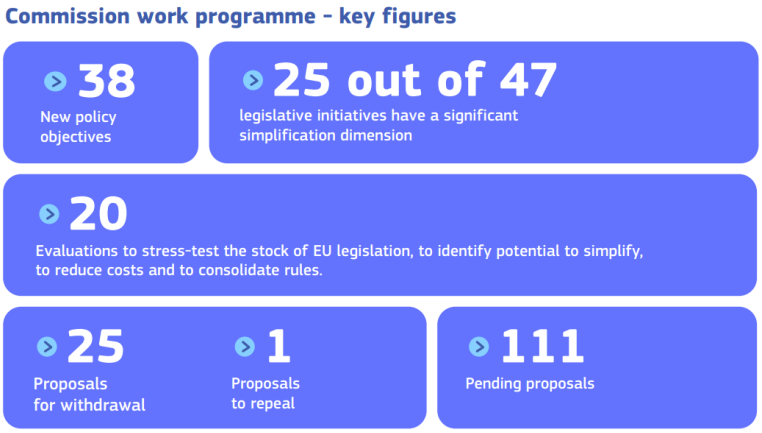
It must focus on ensuring our sovereignty, whether in digital, the economy or security. These are the guiding principles behind this Commission work programme.

It draws on President von der Leyen's Political Guidelines, Mission Letters and the ideas set out in the 2025 State of the European Union address. It is also inspired by consultations with the European Parliament and with Member States. It ensures that we stay the course on all the goals we have collectively agreed upon and respond to the most urgent new priorities. In this spirit, the Commission is ready to work with all EU institutions and stakeholders to deliver on our priorities.

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

Commission work programme 2026

Europe's Independence Moment



To learn more:
https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2414

Number 2

Basel III monitoring report, October 2025

BIS

Basel III risk-based capital ratios increase while leverage ratio and Net Stable Funding Ratio remain stable for large internationally active banks.

Overview of results (unbalanced data set) Table 1

	30 June 2024[1]			31 December 2024		
	Group 1	Of which: G-SIBs	Group 2	Group 1	Of which: G-SIBs	Group 2
Initial Basel III framework						
CET1 ratio (%)	13.4	13.2	18.9	14.0	13.8	18.0
Target total capital shortfalls (€ bn)[2]	0.0	0.0	0.0	0.0	0.0	0.0
TLAC shortfall 2022 minimum (€ bn)	7.3	7.3		8.8	8.8	
Total accounting assets (€ bn)	83,501	62,632	2,752	67,056	45,746	3,289
Leverage ratio (%)[3]	6.1	6.0	6.7	6.2	6.0	6.5
LCR (%)	135.9	133.5	194.1	134.8	131.7	200.8
NSFR (%)	123.6	123.8	137.5	123.7	124.3	135.2
Fully phased-in final Basel III framework (2028)						
Change in Tier 1 MRC at the target level (%)	1.8	1.4	5.2	2.1	1.5	1.3
CET1 ratio (%)	13.0	12.8	17.7	13.4	13.3	16.2
Target capital shortfalls (€ bn); of which:	0.9	0.9	0.0	0.0	0.0	0.0
CET1	0.0	0.0	0.0	0.0	0.0	0.0
Additional Tier 1	0.0	0.0	0.0	0.0	0.0	0.0
Tier 2	0.9	0.9	0.0	0.0	0.0	0.0
TLAC shortfall 2022 minimum (€ bn)	6.8	6.8		5.7	5.7	
Leverage ratio (%)[3]	6.1	6.0	6.8	6.2	6.0	6.5

See Table A.4 for the target level capital requirements. [1] The values for the previous period may differ slightly from those published in the previous report. This is caused by data resubmissions for previous periods to improve the underlying data quality and enlarge the time series sample. [2] These use the 2017 definition of the leverage ratio exposure measure. [3] The leverage ratios reflect temporary exclusions from leverage exposures introduced in some jurisdictions.

Source: Basel Committee on Banking Supervision.

To assess the impact of the Basel III framework on banks, the Basel Committee on Banking Supervision monitors the effects and dynamics of the reforms.

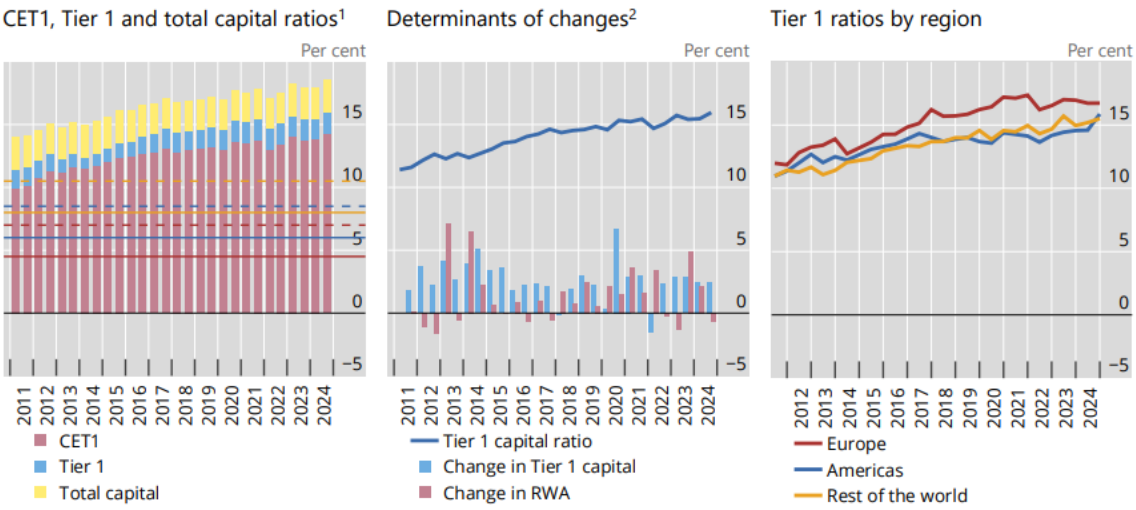
For this purpose, a semiannual monitoring framework has been set up for the risk-based capital ratio, the leverage ratio and liquidity metrics, using data collected by national supervisors on a representative sample of institutions in each country.

Since the end-2017 reporting date, the analyses have also captured the effects of the Committee's finalisation of the Basel III reforms.

This summary is based on aggregate results using data as of 31 December and compares it with the previous reporting period.

Current Basel III capital ratios show a sizeable increase, driven by the Americas

Group 1 banks, balanced data set — Graph 1



[1] The solid lines depict the relevant minimums, the dotted lines the minimums plus the capital conservation buffer. See Table A.4 for the relevant levels. [2] Exchange rates as at the current reporting date.

Source: Basel Committee on Banking Supervision. See the Excel data file for underlying data and sample size.

The Committee believes that the information contained in this summary and the related dashboards will provide relevant stakeholders with a useful benchmark for analysis.

Information considered in the analysis was obtained from voluntary and confidential submissions of data from individual banks and their national supervisors.

At the jurisdictional level, there may be ongoing mandatory data collection, which also feeds into this report.

Data were included for 176 banks, including 116 large internationally active ("Group 1") banks, among them 29 global systemically important banks (G-SIBs) and 59 other ("Group 2") banks.

Members' coverage of their banking sector is very high for Group 1 banks, reaching 100% coverage for some countries, while coverage is lower for Group 2 banks and varies by country.

In general, these analyses do not consider any transitional arrangements such as grandfathering arrangements. Rather, the estimates presented assume full implementation of the Basel III requirements based on data as of 31 December 2024. No assumptions have been made about banks' profitability or behavioural responses, such as changes in bank capital or balance sheet composition, since this date or in the future.

Furthermore, the report does not reflect any additional capital requirements under Pillar 2 of the Basel III framework.

Basel III minimum requirements and buffers — Table A.1

	As of 1 January 2019
Leverage ratio	3.0%
Minimum CET1 ratio	4.5%
Capital conservation buffer	2.50%
G-SIB surcharge	1.0–2.5%
Minimum common equity plus capital conservation buffer	7.0%
Phase-in of deductions from CET1 (including amounts exceeding the limit for DTAs, MSRs and financials)	100%
Minimum Tier 1 capital	6.0%
Minimum total capital	8.0%
Minimum total capital plus capital conservation buffer	10.5%
Capital instruments that no longer qualify as Tier 1 capital or Tier 2 capital	Phased out over 10-year horizon beginning 2013
Liquidity Coverage Ratio	100%
Net Stable Funding Ratio	100%[1]

[1] Note that as of September 2023, a final rule for the Net Stable Funding Ratio is in force in 26 out of 27 Basel Committee member jurisdictions. See Basel Committee on Banking Supervision, *RCAP: Basel III implementation dashboard*, October 2023, www.bis.org/bcbs/implementation/rcap_reports.htm.

To learn more: https://www.bis.org/bcbs/publ/d599.pdf

Number 3

Vigilance Across Borders: The Global Imperative for Audit Quality
George R. Botic, Acting Chair, at the 17th Annual PCAOB International Institute
Washington, DC

Good morning and thank you, Michelle [Wildstein], for the introduction. It is my pleasure to welcome you to Washington, D.C., and to the PCAOB's 17th annual International Institute. I see so many familiar faces, and I am very much looking forward to catching up with old friends and colleagues and making new ones, especially at this evening's reception.

Each year, I always look forward to the informal and engaging discussions that occur in the morning over breakfast, and I am happy to report that the dialogue that I had this morning did not disappoint.

I want to begin by thanking Karen Dietrich and the entire Office of International Affairs for bringing this event to life and for convening such a remarkable group of well recognized and accomplished audit regulators, standard setters, and professionals from around the world. I encourage you to take full advantage of the vast, global expertise in this room over the next few days. This is truly a unique opportunity and a highlight of the year.

I also want to acknowledge that there are both travel and budget considerations for you to be here these few days, and we are grateful for your efforts and do not take them for granted.

Before I continue, please know that my remarks this morning are my own as an individual PCAOB Board Member and do not necessarily reflect the views of the full Board, my fellow Board Members, or the PCAOB's dedicated staff.

Looking back, 2007 proved to be a productive year for global audit oversight and collaboration: The International Forum of Independent Audit Regulators (IFIAR) held its first meeting in Tokyo, and the PCAOB hosted its first International Institute in Washington, D.C.

Since then, as individual regulators, we have grown together to identify shared challenges and risks and then translate them into practical, forward-looking solutions – solutions that have meaningfully strengthened audit oversight across jurisdictions. Through our collaborative oversight activities, including joint inspections, we have demonstrated time and time again that our collective impact is greater than the sum of our individual efforts.

Together, we are not only enhancing audit quality – we are shaping a more resilient and accountable global audit oversight regime. This necessitates our continued commitment and vigilance.

I am always grateful to see how well attended the Institute is. As I was thinking about why the Institute, IFIAR, and other international oversight bodies and gatherings are so critical to what we do, I was reminded of something President Ronald Reagan said in his first inaugural address, "We must act today in order to preserve tomorrow."

That simple truth – of our collective action, forward-thinking, and vigilance – frames why we are gathered here this week. The experiences we will have over the next two days are essential to strengthening investor protection in capital markets around the world.

This morning, I would like to speak about three themes that underscore why global collaboration is critical to protecting investors and the public interest: First, the acceleration of financial and technological change across the financial reporting ecosystem, including with accounting firms; second, the evolution of the PCAOB's role; and, finally, the vigilance that is necessary to ensure consistent audit quality.

Acceleration of Financial and Technological Change Across the Financial Reporting Ecosystem

We are living in a time of rapid change. Markets are volatile. New asset classes and investment vehicles are reshaping the landscape. Valuations can be complex and require specialized skills. And the demand for transparency, accountability, and ethical governance continues to grow.

Investor confidence is a cornerstone of economic resilience, and audit quality is a critical line of defense against material misstatements, fraud, and the erosion of trust.

Ultimately, just as the Institute is a forum for the sharing of ideas, perspectives, and insights, I believe the PCAOB is, and must be, a marketplace of ideas, bringing together diverse voices from other regulators and standard setters, investors, auditors, audit committee members, preparers, and the academic community to candidly discuss perspectives and practices that improve audit oversight and protect investors.

As we convene this marketplace of ideas, there are two emerging trends that I would like to discuss and that deserve our collective focus: private equity investments in accounting firms and the rapid adoption of artificial intelligence in the audit.

These trends have the potential to transform auditing as we know it and require our continued attention.

First, private equity investments and other alternative financing arrangements in accounting firms are reshaping ownership structures. These investments can be used to acquire advanced technologies, streamline operations, and assist in attracting and retaining professionals, which can lead to enhanced audit quality.

But there are concerns from regulators and standard setters around the globe. This summer, the International Ethics Standards Board for Accountants (IESBA) issued a warning about the risks that private equity investments in the audit pose to auditor independence and the potential for conflicts of interest.

Additionally, data from the Dutch Authority for the Financial Markets (AFM) shows the following trends in private equity-backed audits: a decline in statutory auditor involvement, reduced identification of significant risks, and increased threats to independence.

I, too, have my own concerns that the private equity model focused on short-term ownership and possible cost-savings may change long established incentive structures and behaviors within accounting firms and may, over time, undermine the core principles of audit quality.

Having said that, I recognize that many of today's accounting firms face new and additional demands for capital that must be met to remain competitive, and those demands may not be achieved through the traditional partnership structure.

As regulators, we must ensure our oversight remains vigilant as this trend continues.

This vigilance requires engagement with all stakeholders, and in particular, it requires encouraging academic research to ensure we have a comprehensive understanding of not only the challenges and risks, but also the benefits of these investments and structures.

I look forward to hearing more about Professor Maria Borysoff's research and insights on this topic tomorrow morning.

The second trend I want to raise is how the ever-expanding use of artificial intelligence (AI) is transforming the way companies operate and how audits are performed.

AI's rapidly advancing capabilities are already disrupting traditional professional services and business. I will highlight this with two examples:

First, Walmart is using AI-powered chatbots to automate supplier negotiations to reduce costs and increase productivity.

Second, AI is also upending the model used by consulting firms as the work of junior consultants – gathering data, analyzing it, and modeling scenarios in support of senior consultants – can now be done by AI. In fact, McKinsey's proprietary AI system is used by more than 72% of its workforce, reducing research and synthesis time by approximately 30%.

More specific to auditing, a recent study found that 70% of U.S. audit professionals say they use AI weekly in their role, and more than three-quarters of firms plan to increase their AI investments.

Furthermore, an Accounting Today survey shows that 72% of respondents are "comfortable using technology for work that traditionally required human effort" with more than half of respondents reporting that "AI makes them more effective." A challenge then lies in the deployment of this technology and what exactly it is being used for.

These examples illustrate how AI is already reshaping core functions across different businesses, but what lies ahead may be even more transformative. While still theoretical, the possibility of artificial super intelligence emerging within the next decade, as predicted by OpenAI CEO Sam Altman, signals just how rapidly this technology is evolving. There is a critical balancing act of embracing technology while keeping the human-in-the-loop, or as I recently heard someone say in a meeting, keeping the human-in-the-lead.

So, as AI tools begin to influence judgments traditionally made by humans, auditors must grapple with how to preserve due professional care, professional skepticism, independence, and accountability in a rapidly changing digital landscape.

In summary, I know private equity and AI are topics many of us are exploring in our own organizations. In addition, IFIAR has been working on topics related to technology and AI through its technology task force and has recently established another task force to consider alternative investments in accounting firms. I look forward to hearing the results of their continued work.

Additionally, we will have an opportunity to learn more during a technology panel later today and a discussion on private equity tomorrow.

Evolution of the PCAOB's Role

I would now like to move to the second theme, which is the evolution of the PCAOB's role. Our mission is clear: to oversee the auditors of public companies and broker-dealers to protect the interests of investors and further the public interest in the preparation of informative, accurate, and independent audit reports.

To exercise our statutory oversight effectively, the PCAOB has conducted inspections in more than 50 jurisdictions and has entered into more than 28 bilateral agreements. These relationships enable joint inspections, enforcement actions, when necessary, and shared practices and experiences, and they help create a united front in the best interest of the investors and the public.

Building on our presence across the world, the PCAOB's inspection program reflects the depth and breadth of our global oversight activities. In 2024, our inspectors inspected 171 firms and reviewed portions of 803 audits of public

companies including, in cooperation with many of you, inspections of 78 non-U.S. firms, in which we reviewed portions of 221 audits.

These inspection results not only reflect the extent of our global oversight, they also inform and reinforce the evolution of our standards, ensuring our standards remain responsive to emerging risks and aligned with the realities of a dynamic audit environment.

As the theme for this year's Institute suggests, we are focused on accounting firms' systems of quality control. Although its implementation has been delayed until next year, QC 1000, A Firms' System of Quality Control 12, is designed to strengthen firms' quality control systems and promote accountability and further audit quality.

I think we will all agree that an accounting firm's system of quality control is the foundation for consistently performing high quality audits.

Both QC 1000 and ISQM 1 share a common goal to elevate audit quality through proactive, scalable systems. We welcome the opportunity to learn from you about how the new QC standard functions across jurisdictions.

As we consider how systems of quality control are implemented, it is important to remember that quality control is just one piece of the larger puzzle.

Because while strong quality control systems are essential, they are ultimately in service to something broader: audit quality itself. That brings me to another area I want to highlight – how we define audit quality, and why that definition matters.

I believe the PCAOB should endeavor to create a definition of audit quality that can act as an anchor for participants in the financial reporting ecosystem. Some of you here today have already established such a framework, and we would welcome your insights and feedback.

Vigilance Necessary to Advance Audit Quality

Our third and last theme is the need for our vigilance. As global momentum moves toward stronger standards, as evidenced by QC 1000 and ISQM 1, shared accountability reflects the importance of global collaboration.

To this point, an academic paper identified the work that we collectively do as audit regulators as "one of the most significant changes in the history of the auditing profession."

Audit oversight is global – this room is a testament to that – and the auditing profession finds itself at a crossroads: where innovation, investment, and international complexity converge.

Whether it is the influence of private equity or the rise of AI, we face shared challenges that demand shared solutions.

That is why this Institute matters. The PCAOB wants to hear what is happening in your jurisdictions, how you are approaching emerging risks, and where we can learn from one another. We know that trust is built through transparency, consistency, and dialogue. And we are committed to all three.

A Shared Future

In closing, I want to go back to President Reagan's urge to "act today to preserve tomorrow."

Meeting that call requires our collective vigilance. So often throughout history, economic calamity has struck when we least expect it. Though, in the cold air of hindsight, the problem almost always looked obvious.

This call to action resonates deeply in our work: protecting investors and safeguarding the future of auditing through the choices we make today. And together, our collective work helps to enable a financial reporting ecosystem that is resilient and responsive.

Thank you again for your presence this week. I look forward to the conversations ahead, and now I would like to invite my fellow Board Members to join me on stage for our panel discussion and your questions and comments – all are welcome.

Note: George R. Botic was designated as Acting Chair of the Public Company Accounting Oversight Board by the Securities and Exchange Commission on July 21, 2025. He was appointed as a Board Member of the Public Company Accounting Oversight Board by the SEC in September 2023 and sworn in on October 25, 2023. His current term expires on October 24, 2028.

To learn more:
https://pcaobus.org/news-events/speeches/speech-detail/vigilance-across-borders--the-global-imperative-for-audit-quality

Number 4

Opening Remarks

Michelle W. Bowman, Vice Chair for Supervision of the Board of Governors of the Federal Reserve System, at the Economic Growth and Regulatory Paperwork Reduction Act Outreach Meeting, Federal Reserve Bank of Kansas City, Kansas City, Missouri

Good morning and welcome to the third public outreach meeting hosted by the federal banking agencies related to the Economic Growth and Regulatory Paperwork Reduction Act (EGRPRA).

The bank regulatory system has grown extensively in recent years and has become overly complicated with often conflicting and overlapping requirements.

The growth of these requirements has imposed unnecessary and significant costs on banks and their customers.

I have spoken about my principles for supervision and regulation, which will continue to guide my approach to supervision and the bank regulatory framework.

At the core of these principles is pragmatism, which focuses on first identifying the problem each new and existing regulation intends to solve and then reviewing and updating regulations as industries and conditions change.

Once we have identified a need for reform, or a problem to be solved, our next task is to conduct a careful analysis of the intended and unintended consequences of any proposed policy solution and to consider alternative approaches that lead to lower costs or better outcomes.

The EGRPRA process is the opportunity to do just this—take a step back and review our frameworks with fresh eyes to eliminate unnecessary and outdated regulations and reduce burden. The bank regulatory framework must strike a balance between encouraging economic growth and innovation while guaranteeing the safety, soundness, and stability of the banking system.

One of the primary goals of the EGRPRA process is to maintain the regulatory framework to ensure it continues to be fit for purpose. As I've noted previously, system maintenance is something we should embrace. When regulators establish rules and guidance, they devote significant time, resources, and analysis to evaluate the costs and benefits of new proposals.

However, insufficient focus is given to updating and refining these frameworks. Ideally, regulators should be adapting the regulatory structure to ensure the existing plumbing continues to work, considering how different regulations interact with each other, reflecting changes in the evolving financial landscape, or accommodating innovations such as new financial products, services, or market participants.

So, our work to maintain an effective bank regulatory framework is never really complete. If regulators do not consistently reassess what is already in place, it can prevent us from meeting our statutory obligation to promote a safe and sound banking system that enables banks to serve their customers effectively and efficiently.

Over time, some of our regulations have unduly restrained the activities that banks can engage in, incentivizing banks to limit those activities and pushing those functions outside of the banking system. We need to ask whether this is appropriate. Similarly, the buildup of complexity in our regulatory system is also felt most acutely by community banks.

When our regulatory system is not appropriately tailored to the size, risk, complexity, and business model of the institutions we supervise and regulate, we impede the effectiveness of their operations. This can result in preventing banks from providing competitive products and services, innovating, and engaging in appropriate risk-taking. Incorporating graduated requirements avoids disproportionately burdening smaller institutions.

The current EGRPRA review is the third time the agencies have undertaken a comprehensive review of the bank regulatory system. The two prior reviews were underwhelming, resulting in no reduction in regulatory burden. This is an unacceptable outcome.

We must take this process seriously, and through it, actually identify opportunities for change that will have lasting impact. We are implementing the current process to provide meaningful engagement for stakeholders to identify regulatory changes that result in less complexity, lower compliance costs, and increased efficiency while also maintaining safety and soundness.

As part of the current review, the agencies have issued four Federal Register notices and held two virtual outreach meetings. We have received comments from many stakeholders including banks, trade groups, and community organizations.

This broad range of commenters demonstrates the important role of the banking system in the lives of all Americans. We must strike the right balance and be responsive to public comments and through outreach meetings like this meeting today.

A significant portion of the comments received so far highlight areas of regulation that I have targeted for revisiting. Many of the Board's regulations have not been comprehensively reviewed or updated in more than 20 years. Given the dynamic nature of the banking system and how the economy and banking industry have

evolved over that period, we should update and simplify many of the Board's regulations, including thresholds for applicability and benchmarks. These thresholds should also be indexed to account for economic growth and inflation.

Commenters have offered suggestions to address a number of areas, including issues with the Board's supervisory framework, regulatory capital, and the applications process. They have also discussed more specific issues ranging from outdated guidelines on loans to insiders, bank activities, and anti-money laundering requirements.

Many commenters have also remarked on the excessive burden created by information and regulatory data collections, with an emphasis on the Call Report and other information collections. We are carefully considering these comments and are evaluating ways to address related unnecessary regulatory burdens.

With this feedback in mind, the Board is already working to update and streamline many of these requirements. For example, on regulatory capital, we are pursuing several initiatives, including considering modifications to the Community Bank Leverage Ratio, changes to our stress testing process to reduce volatility of capital requirements, and making proposed changes to the enhanced supplementary leverage ratio.

The Board also recently issued an FAQ to provide transparency and clarify the considerations a mutual banking organization should evaluate when proposing to issue a mutual capital instrument. We are also prioritizing work to assist in the fight against fraud and considering ways to streamline the mergers, acquisitions, and de-novo formations review and approval process.

The Board is also committed to refocusing our supervisory process on material financial risks rather than procedural or documentation issues and identifying and eliminating the hidden costs and extra-regulatory burdens implemented through supervision.

As part of this initiative, the Board has initiated changes to our large bank ratings framework to better align it with other supervisory ratings systems and ensure large banks' ratings reflect their financial conditions and risks. In addition, we and the other FFIEC agencies are reviewing the CAMELS ratings system, which is long past due for reform.

The Board has also taken steps to ensure our supervisory framework is supportive of innovation in the banking system, and we have ended the use of reputational risk in our supervisory program to guarantee fair access to the banking system for all Americans.

Looking ahead, the Board will review a broad set of issues to ensure our regulatory framework and supervisory approaches are appropriately tailored and transparent. Through the EGRPRA process, we have a meaningful opportunity to reduce unnecessary and outdated regulatory requirements. Our responsibility is to promote safety and soundness and consider the broader context of promoting

an effective and efficient banking system that supports market functioning and encourages economic growth, business creation and expansion, and opportunity.

I continue to prioritize outreach to banks of all sizes, especially community banks, because your voice must be a part of the conversation in Washington to shape a regulatory framework that fosters growth and innovation. We look forward to engaging on your comments and concerns and constructive ideas for further improvements.

Thank you for your participation.

To learn more:
https://www.federalreserve.gov/newsevents/speech/bowman20251030a.htm

Number 5

Commission preliminarily finds TikTok and Meta in breach of their transparency obligations under the Digital Services Act

The European Commission preliminarily found both TikTok and Meta in breach of their obligation to grant researchers adequate access to public data under the Digital Services Act (DSA). The Commission also preliminarily found Meta, for both Instagram and Facebook, in breach of its obligations to provide users simple mechanisms to notify illegal content, as well as to allow them to effectively challenge content moderation decisions.

Data access for researchers

The Commission's preliminary findings show that Facebook, Instagram and TikTok may have put in place burdensome procedures and tools for researchers to request access to public data. This often leaves them with partial or unreliable data, impacting their ability to conduct research, such as whether users, including minors, are exposed to illegal or harmful content.

Allowing researchers access to platforms' data is an essential transparency obligation under the DSA, as it provides public scrutiny into the potential impact of platforms on our physical and mental health.

Notice and Action mechanisms

When it comes to Meta, neither Facebook nor Instagram appear to provide a user-friendly and easily accessible 'Notice and Action' mechanism for users to flag illegal content, such as child sexual abuse material and terrorist content. The mechanisms that Meta currently applies seems to impose several unnecessary steps and additional demands on users. In addition, both Facebook and Instagram appear to use so-called 'dark patterns', or deceptive interface designs, when it comes to the 'Notice and Action' mechanisms.

Such practices can be confusing and dissuading. Meta's mechanisms to flag and remove illegal content may therefore be ineffective. Under the DSA, 'Notice and Action' mechanisms are key to allowing EU users and trusted flaggers to inform online platforms that certain content does not comply with EU or national laws. Online platforms do not benefit from the DSA's liability exemption in cases where they have not acted expeditiously after being made aware of the presence of illegal content on their services.

Content moderation appeals

The DSA also gives users in the EU the right to challenge content moderation decisions when platforms remove their content or suspend their accounts. At this stage, the decision appeal mechanisms of both Facebook and Instagram does not

appear to allow users to provide explanations or supporting evidence to substantiate their appeals. This makes it difficult for users in the EU to further explain why they disagree with Meta's content decision, limiting the effectiveness of the appeals mechanism.

The Commission's views related to Meta's reporting tool, dark patterns and complaint mechanism are based on an in-depth investigation, including co-operation with Coimisiún na Meán, the Irish Digital Services Coordinator.

These are preliminary findings which do not prejudge the outcome of the investigation.

Next steps

Facebook, Instagram and TikTok now have the possibility to examine the documents in the Commission's investigation files and reply in writing to the Commission's preliminary findings. The platforms can take measures to remedy the breaches. In parallel, the European Board for Digital Services will be consulted.

If the Commission's views are ultimately confirmed, the Commission may issue a non-compliance decision, which can trigger a fine of up to 6% of the total worldwide annual turnover of the provider. The Commission can also impose periodic penalty payments to compel a platform to comply.

New possibilities for researchers will open up on 29 October 2025, as the delegated act on data access comes into force. This act will grant access to non-public data from very large online platforms and search engines, aiming to enhance their accountability and identify potential risks arising from their activities.

Background

The Commission's preliminary findings are part of the Commission's formal proceedings launched into Meta, and formal proceedings to investigate TikTok, under the DSA. The Commission continues its investigation into other potential breaches that are part of these ongoing proceedings. These formal proceedings under the DSA are distinct from ongoing investigations against Facebook, Instagram and TikTok concerning compliance with other relevant EU law.

To learn more:
https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2503

Digital Services Act (DSA), from Cyber Risk GmbH:
https://www.eu-digital-services-act.com/

What is the Digital Services Act (DSA)?

The Digital Services Act is the most important and most ambitious regulation in the world in the field of the protection of the digital space against the spread of illegal content, and the protection of users' fundamental rights. There is no other legislative act in the world having this level of ambition to regulate social media, online marketplaces, very large online platforms (VLOPs) and very large online search engines (VLOSEs). The rules are designed asymmetrically: Larger intermediary services with significant societal impact (VLOPs and VLOSEs) are subject to stricter rules.

After the Digital Services Act, platforms will not only have to be more transparent, but will also be held accountable for their role in disseminating illegal and harmful content.

Amongst other things, the DSA:

1. Lays down special obligations for online marketplaces in order to combat the online sale of illegal products and services;

2. Introduces measures to counter illegal content online and obligations for platforms to react quickly, while respecting fundamental rights;

3. Protects minors online by prohibiting platforms from using targeted advertising based on the use of minors' personal data as defined in EU law;

4. Imposes certain limits on the presentation of advertising and on the use of sensitive personal data for targeted advertising, including gender, race and religion;

5. Bans misleading interfaces known as 'dark patterns', and practices aimed at misleading.

Stricter rules apply for **very large** online platforms and search engines (VLOPs and VLOSEs), which will have to:

1. Offer users a system for recommending content that is not based on profiling;

2. Analyse the systemic risks they create: Risks related to the dissemination of illegal content, negative effects on fundamental rights, on electoral processes and on gender-based violence or mental health.

Number 6

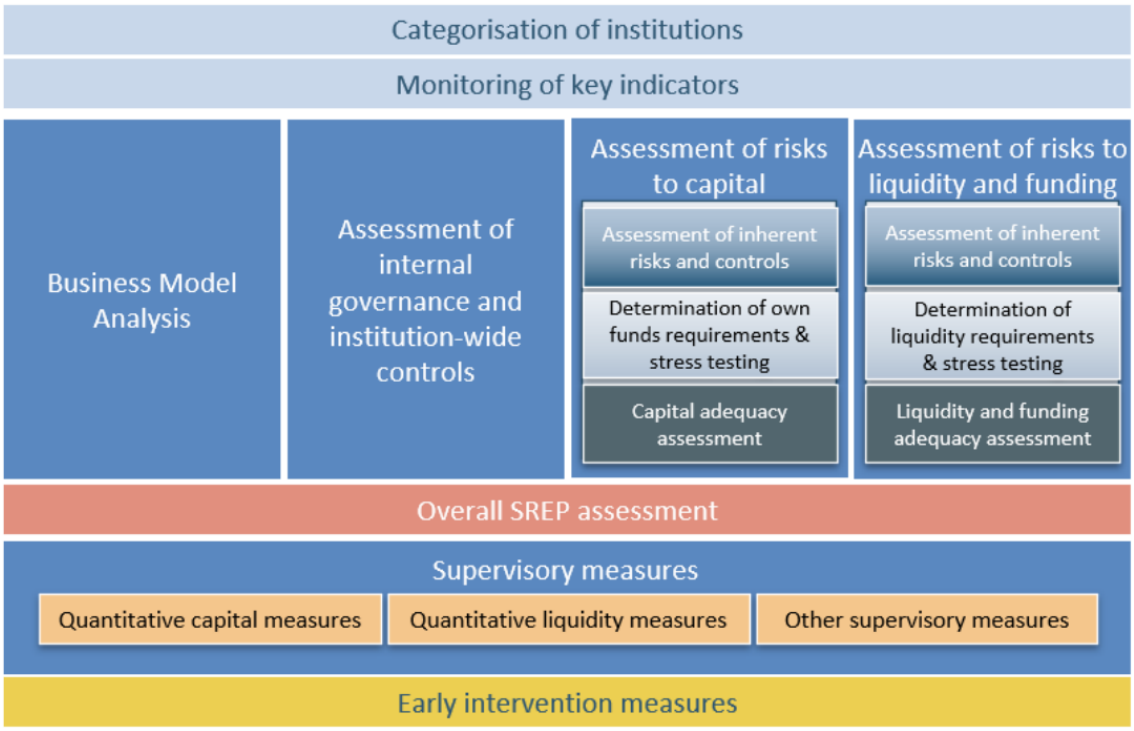
The EBA consults on revised Guidelines on supervisory review and evaluation process and supervisory stress testing

The European Banking Authority (EBA) launched a public consultation on its revised Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP) and supervisory stress testing.

The revision forms are part of the EBA's ongoing efforts to simplify and enhance the efficiency of the EU supervisory framework, while supporting a risk-focused and effective supervision.

The draft revised Guidelines bring changes across all the main SREP elements and further clarify the ongoing nature of the SREP to enhance the rationalisation of the supervisory process.

Figure 1: Overview of the SREP framework

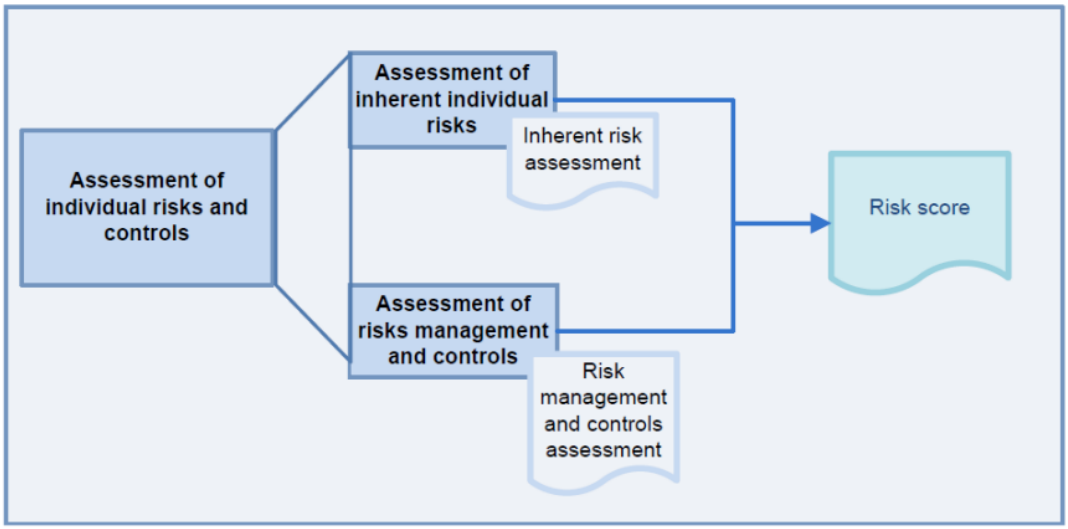


They enhance proportionality aspects taking into account the peer review on the application of proportionality in the SREP and the relevant recommendations of the EBA's Advisory Committee on Proportionality (ACP).

The draft revised Guidelines encompass the new CRD VI mandates on output floor and third-country branches, align with the interest rate risks for banking

book (IRRBB) and credit spread risk arising from non-trading book activities (CSRBB) package and incorporate ESG factors and operational resilience.

Figure 2. Assessment workflow for risks to capital



The revisions also reflect lessons learned from the practical application of the SREP Guidelines since 2016 through:

- placing emphasis on supervisory effectiveness by providing a clearer link between supervisory measures and assessment areas and introducing a high-level and flexible escalation framework for supervisory actions;
- streamlining while enhancing the liquidity and funding assessments;
- further clarifying the communication of the SREP outcomes; and
- enhancing the focus on ICT risk assessment by incorporating the Digital Operational Resilience Act (DORA) framework and existing Guidelines on ICT risk assessment under the SREP (to be repealed) as recommended by the respective peer review.

Consultation process

Comments to the consultation paper can be sent by clicking on the "send your comments" button on the EBA's consultation page. The deadline for the submission of comments is 26 January 2026.

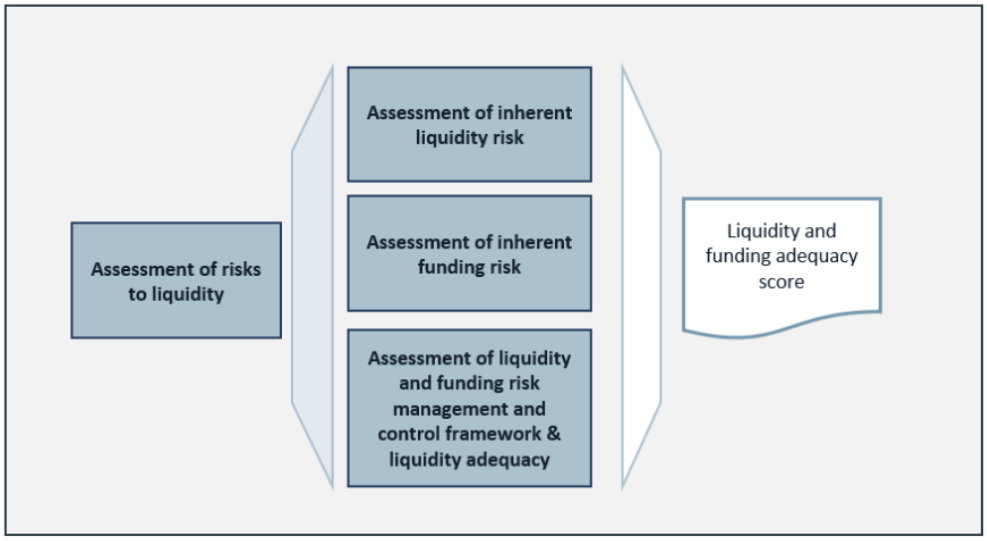
The EBA will hold a virtual public hearing on 4 December from 10:00 to 12:00 - Paris time. The EBA invites interested stakeholders to register using this link by 1 December (16:00 CET). The dial-in details will be communicated to those who have registered for the meeting.

Legal basis

These draft revised Guidelines have been developed on the basis of Article 107(3) of Directive 2013/36/EU, which mandates the Authority to further specify the common procedures and methodologies for the SREP, in accordance with Article 48n(6)a of Directive 2013/36/EU, which mandates the Authority to further specify the common procedures and methodologies for the SREP and for the assessment of the treatment of material risks of third-country branches, and in accordance with Article 104a(7) of Directive 2013/36/EU, which mandates the Authority to further specify the operationalisation of the output floor.

The revised Guidelines will apply to competent authorities – as defined in Article 4(2), points (i) and (viii) of Regulation (EU) No 1093/2010 – across the EU. Once the revised Guidelines will enter into force, the current SREP Guidelines and the Guidelines on ICT risk assessment under the SREP will be repealed.

Figure 3. Elements of the assessment of risks to liquidity and funding



To learn more:
https://www.eba.europa.eu/sites/default/files/2025-10/c5f0c511-b9cc-44fb-bb8a-bf8892953db4/Consultation%20paper%20on%20revised%20Guidelines%20on%20SREP%20and%20supervisory%20stress%20testing.pdf

Number 7

Eurosystem moving to next phase of digital euro project

EUROPEAN CENTRAL BANK
EUROSYSTEM

- New phase will ensure technical readiness for first issuance
- If legislation in place in the course of 2026, a pilot exercise could start in 2027 and the Eurosystem should be ready for a potential first issuance of the digital euro during 2029
- Preparation phase begun in November 2023 has successfully concluded

The Governing Council of the European Central Bank (ECB) has decided to move to the next phase of the digital euro project. This decision follows the successful completion of the preparation phase, launched by the Eurosystem in November 2023, which laid the foundations for issuing a digital euro.

The Governing Council's decision aligns with European leaders' request to accelerate progress on the digital euro, as recently stated at the October 2025 Euro Summit.

A digital euro will preserve Europeans' freedom of choice and privacy and protect Europe's monetary sovereignty and economic security. It will foster innovation in payments and help make European payments competitive, resilient and inclusive.

The Eurosystem will implement its preparations flexibly, in line with calls from euro area leaders for the Eurosystem to be ready for a potential digital euro issuance as soon as possible, while also recognising that the legislative process has not yet been completed.

The ECB Governing Council's final decision on whether to issue a digital euro, and on what date, will only be taken once the legislation has been adopted.

Under the assumption that European co-legislators will adopt the Regulation on the establishment of the digital euro in the course of 2026, a pilot exercise and initial transactions could take place as of mid-2027. The whole Eurosystem should then be ready for a potential first issuance of the digital euro during 2029.

"The euro, our shared money, is a trusted sign of European unity," said ECB President Christine Lagarde. "We are working to make its most tangible form – euro cash – fit for the future, redesigning and modernising our banknotes and preparing for the issuance of digital cash."

As payment habits evolve, and cash payments decline compared with digital transactions, the need for a public digital means of payment – complementary to cash – has become increasingly urgent. The digital euro will complement cash and

bring its benefits – simplicity, privacy, reliability, availability across the whole euro area – to digital payments.

Along with the Regulation on the establishment of the digital euro, the ECB is also supporting the European Commission's proposal to reinforce the right to pay with cash.

The Eurosystem will focus on three main areas:

1. technical readiness: developing the digital euro's technical foundations, including initial system set-up and piloting;
2. market engagement: collaborating with payment providers, merchants and consumers to finalise the rulebook, conduct user research and test the system through pilot activities;
3. legislative process support: continue providing technical input to EU co-legislators and assist the legislative process as required.

"This is not just a technical project but a collective effort to future-proof Europe's monetary system," said ECB Executive Board member Piero Cipollone, who chairs the High-Level Task Force on a digital euro. "A digital euro will ensure that people enjoy the benefits of cash also in the digital era. In doing so, it will enhance the resilience of Europe's payment landscape, lower costs for merchants, and create a platform for private companies to innovate, scale up and compete."

Transparency and close cooperation with stakeholders have been – and will continue to be – fundamental to the project. The Eurosystem has benefited greatly from feedback from European decision-makers, market participants and potential users, and will continue to engage actively with a wide range of stakeholders.

The Eurosystem's continued preparation for a digital euro will be implemented flexibly, ensuring alignment with the legislative process. To this end, work will be structured in modules to enable gradual scaling and limit financial commitments.

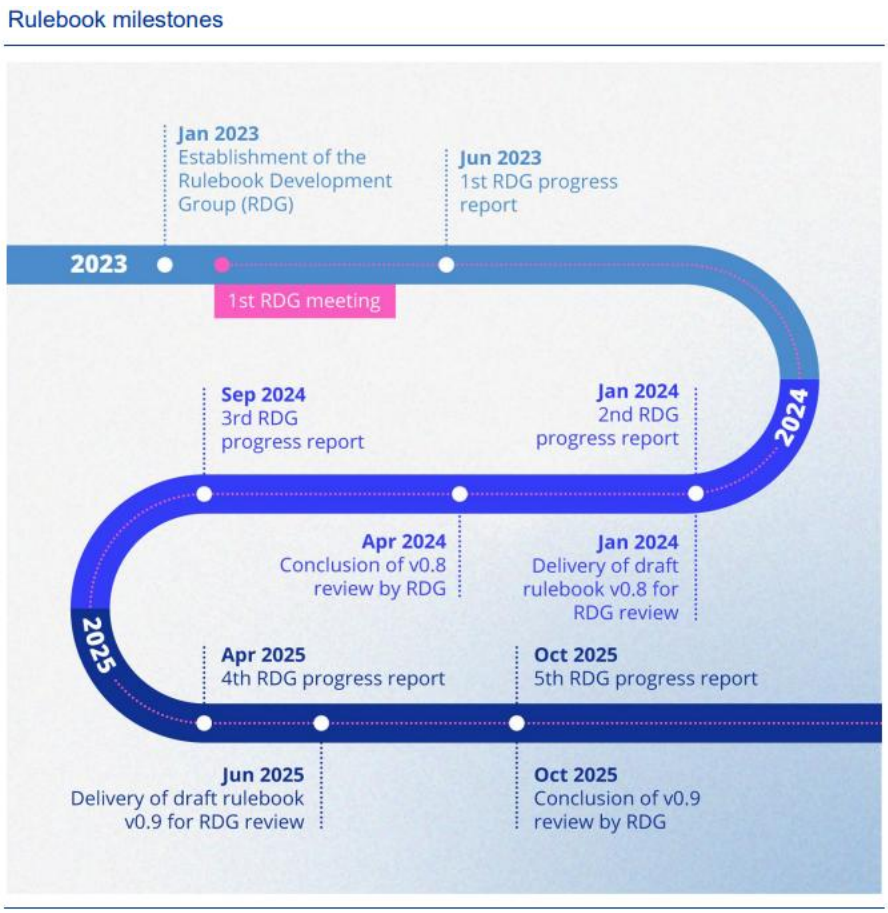
The final cost of a digital euro – for both its development and operation – will depend on its final design, including components and related services that need to be developed.

As a result of the work done in the preparation phase, the total development costs, comprising both externally and internally developed components, are estimated at around €1.3 billion until the first issuance, which is currently expected during 2029. Subsequent annual operating costs are projected to be approximately €320 million per year from 2029.

The Eurosystem would bear these costs, as it does for producing and issuing euro banknotes – which, like the digital euro, are a public good. As in the case of banknotes, these costs are expected to be compensated by the generated seigniorage – even if digital euro holdings were small compared with banknotes in circulation.

The conclusion of the preparation phase marks an important transition in the digital euro project. Building on the insights gained during the investigation phase conducted from 2020 to 2023, we moved towards refining its practical design. Key achievements include:

(i) the development of the draft digital euro scheme rulebook,



(ii) the selection of providers for digital euro components and related services,

(iii) the successful running of an innovation platform for experimentation with market participants, as well as

(iv) the investigation by a technical workstream into the fit of the digital euro in the payment ecosystem.

The latter, conducted by the ECB and market participants via the Euro Retail Payments Board, concluded that a digital euro could foster further competition in the European payments market. Besides directly benefiting from distributing the digital euro, banks and other payment service providers could leverage its open standards to expand their reach across the euro area without needing their own acceptance networks. They would also be able to co-badge the digital euro with existing payment solutions.

The ECB provided technical input to co-legislators on request, thereby supporting the legislative process.

This input demonstrated that the costs of the digital euro for banks will be contained – these costs will be close to the European Commission's initial estimates and similar to those incurred for the implementation of the Payment Services Directive. It also showed that safeguards built into the design of the digital euro (such as holding limits) would ensure that it does not create financial stability risks.

To ensure that the digital euro is designed to meet the needs of European citizens and merchants, the Eurosystem conducted extensive user research targeting vulnerable consumers and small merchants. The findings – available in a separate report published today – show the need for a simple, reliable and secure payment experience.

These results reaffirm the ECB's commitment to developing a digital euro that works for everyone and advances Europe's financial evolution – designed to empower citizens, support innovation and strengthen the resilience of our monetary system.

To learn more:
https://www.ecb.europa.eu/press/pr/date/2025/html/ecb.pr251030~8c5b5beef0.en.html

Number 8

The transformation of the life insurance industry: systemic risks and policy challenges

BIS

The life insurance industry has undergone a profound structural transformation since the Great Financial Crisis, amid a prolonged period of exceptionally low interest rates and evolving regulatory frameworks.

This paper examines the systemic risks and policy challenges emerging from this transformation, with a particular focus on the growing involvement of private equity firms, the shift in investment strategies towards riskier and opaque assets, increased use of derivatives and greater reliance on asset-intensive reinsurance, often through offshore jurisdictions.

Standard risk metrics indicate that the sector's systemic importance has risen, notably in the Americas and Asia, due to heightened interconnectedness with the broader financial system.

Liquidity risks have become more pronounced, stemming from greater use of short-term funding, policy surrenders, and use of derivatives, while governance complexities and opacity in asset valuation further complicate supervision.

Several measures could be considered to address these challenges, such as enhancing supervisory frameworks and disclosures, prudential charges to

mitigate concentration risk and liquidity risk, harmonisation of international standards and complementing supervision with a macroprudential perspective to monitor and address concentration risks and financial interlinkages at the system level.

Overall, while the sector has demonstrated adaptability and resilience, its growing complexity and interconnectedness highlights the need for vigilant regulation to safeguard financial stability and preserve the sector's critical role in the financial system.

To learn more: https://www.bis.org/publ/bppdf/bispap161.pdf

Number 9

Don't take BADCANDY from strangers – How your devices could be implanted and what to do about it

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Cyber actors are installing an implant dubbed 'BADCANDY' on Cisco IOS XE devices that are vulnerable to CVE-2023-20198. Variations of the BADCANDY implant have been observed since October 2023, with renewed activity notable throughout 2024 and 2025.

BADCANDY is a low equity Lua-based web shell, and cyber actors have typically applied a non-persistent patch post-compromise to mask the device's vulnerability status in relation to CVE-2023-20198. In these instances, the presence of the BADCANDY implant indicates compromise of the Cisco IOS XE device, via CVE-2023-20198.

The BADCANDY implant does not persist following a device reboot however, where an actor has accessed account credentials or other forms of persistence, the actor may retain access to the device or network. The patch for CVE-2023-20198 must be applied to prevent re-exploitation. Access to the web user interface should also be restricted if enabled (see the General Hardening section below).

Since July 2025, ASD assesses over 400 devices were potentially compromised with BADCANDY in Australia. As at late October 2025, there are still over 150 devices compromised with BADCANDY in Australia.

CVE-2023-20198

This critical vulnerability affects the web user interface (UI) feature of Cisco IOS XE Software. Exploitation of this vulnerability could allow a remote, unauthenticated user to create a highly privileged account on the vulnerable system, allowing them to take control of the system.

This vulnerability has been leveraged by actors such as SALT TYPHOON and was one of the top routinely exploited vulnerabilities in 2023.

ASD is aware of ongoing exploitation.

Actor attribution

While any actor can use this implant, ASD believes that criminal and state sponsored cyber actors may leverage the BADCANDY implant. Cyber actors are known to re-exploit previously compromised devices where the device has not been patched and the interface has been left exposed to the internet. This presents an ongoing risk to Australian networks.

ASD's response

ASD has sent victim notifications to entities via their service provider if ASD cannot determine the system operator. These notifications contain instructions to patch and reboot the device, perform hardening and, conduct incident response on any impacted devices.

ASD will continue to conduct victim notifications to ensure system operators are aware that their device has been compromised.

To learn more:
https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/badcandy

Number 10

Dissecting YouTube's Malware Distribution Network

Key Points

- Check Point Research uncovered and analyzed the YouTube Ghost Network, a sophisticated and coordinated collection of malicious accounts operating on YouTube. These accounts systematically take advantage of YouTube's features to promote malicious content, ultimately distributing malware while creating a false sense of trust among viewers.

- Our investigation identified and reported more than 3,000 malicious videos associated with this network. The majority of these videos have been removed, significantly reducing the threat to the broader digital ecosystem. The network appears to be active at least since 2021, maintaining a steady output of malicious content each year. Notably, in 2025, the creation of such videos has tripled, highlighting both the scalability and increasing effectiveness of this malware distribution campaign.

- The network primarily targets the "Game Hacks/Cheats" and "Software Cracks/Piracy" categories, areas that continue to attract large numbers of potential victims. It is important to emphasize that the use of cracked software is illegal and that such versions frequently contain hidden malware. The most viewed malicious video in our dataset targets Adobe Photoshop, with 293,000 views and 54 comments, while the second most viewed targets FL Studio, with 147,000 views.

- Prior to the disruption of the Lumma infostealer between March and May 2025, Lumma was the most frequently distributed malware within this network. Following this disruption, we observed a shift in threat actor tactics, with Rhadamanthys becoming the preferred infostealer. Overall, the majority of malware distributed via the YouTube Ghost Network consists of information-stealing malware (infostealers), posing a significant risk to user credentials and sensitive data.

To learn more: https://research.checkpoint.com/2025/youtube-ghost-network/

Disclaimer

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

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

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

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

This information:

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

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

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

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

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

- is in no way constitutive of interpretative;

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

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

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

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

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

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

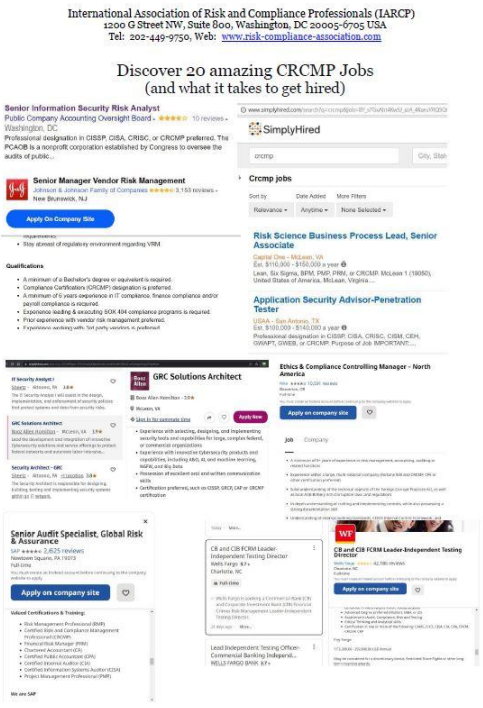
To learn more: https://www.risk-compliance-association.com/Privacy.htm

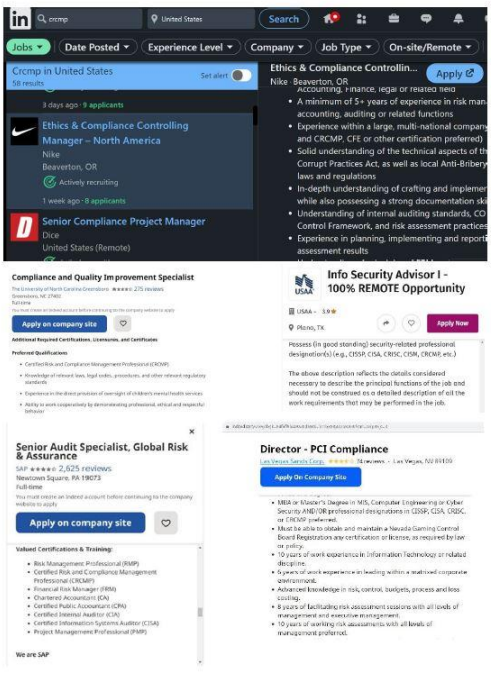
Our training and certification programs:

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

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

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





2. Advanced Specialization, Certified Risk and Compliance Management Professional in Hybrid Risk and Resilience Management - CRCMP(HR²M), online training and certification program. You may visit: https://www.risk-compliance-association.com/CRCMP_HR2M.htm

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

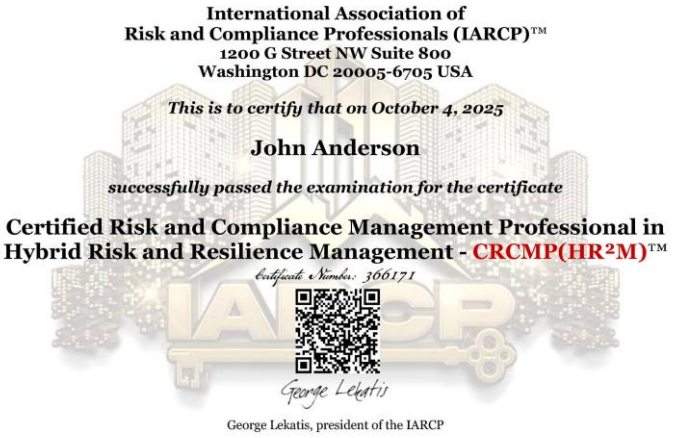
1. Moves from traditional risk and compliance frameworks into the management of multi-vector, cross-domain, and asymmetric threats that transcend conventional boundaries.

2. Develops expertise in hybrid risk governance.

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

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

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



Enrollment in the CRCMP(HR²M) program is restricted to professionals who have already passed the Certified Risk and Compliance Management Professional (CRCMP) exam.

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

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

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

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

Overview

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

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

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

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

Overview

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

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

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

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

Overview

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

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

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

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

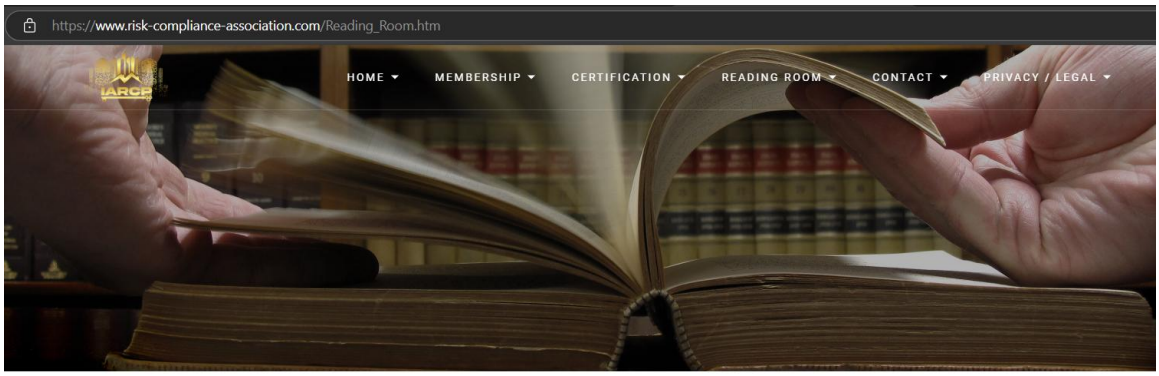
Overview

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

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

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

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



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

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

You may contact:

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

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