Monday, October 20, 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.

Normally, when we hear the word spillover, we think of our morning coffee spilling over the desk. In risk management it's a little messier, and unfortunately, we can't just wipe it away with a napkin.

The term describes how an incident, shock, or vulnerability in one domain produces secondary and unintended consequences in other domains.
We may have a financial spillover, for example, when a bank triggers liquidity shortages in other institutions. Hybrid risks often emerge through spillovers across domains. In other words, spillovers transform what appears to be an isolated breach into hybrid risk that cuts across technology, governance, law, and geopolitics.

Spillover risk is the risk that an adverse event, disruption, or liability gives rise to consequential, indirect, secondary impacts on other activities, entities, sectors, or jurisdictions. Such impacts may include financial loss, operational disruption, regulatory exposure, reputational damage, or legal liability affecting parties not directly involved in the originating event.

Spillover risk often involves:

(i) the propagation of harm through contractual relationships, shared technological or operational infrastructures, or interdependent legal obligations.

(ii) the transmission of risk across borders or regulatory regimes, where such transmission was not expressly intended or contractually assumed by the initially affected party.

But how can we manage spillover risk?

First, we must map interdependencies. If risk leads to exposure, interdependency is the channel along which that exposure travels, and the amplifier that converts a local disturbance into a systemic one.

An interdependency map is a representation of how critical services depend on enabling capabilities, and how those capabilities depend on specific people, facilities, systems, data, and third parties.

Mapping interdependencies reveals unpleasant truths, but those truths exist whether or not they are drawn. It surfaces the connective tissue that allows a business to function but also exposes how easily that function can break.

Unfortunately, this map is a mirror that reflects things many leaders would prefer not to see. It reveals concentrations that contradict diversification claims.

That's the equivalent of mixing drinks at a bar, vodka tonic, vodka soda, bloody mary, vodka cranberry, screwdriver, vodka martini. On paper, it sounds like variety. But if the vodka runs out, our diversification collapses faster than our diet at an all-you-can-eat buffet.

Concentration is often masquerading as efficiency. Interdependency mapping reveals the cumulative result of these *optimizations*. In network terms they are single points of failure that are tempting to ignore, especially when cost savings are celebrated.

When we trace a critical service through its enabling dependencies, we identify precisely which counterparties process which categories of data, in which jurisdictions, under which contracts, and subject to which supervisory regimes.

Interdependency mapping assigns ownership not only to assets but to the relationships between them. Someone must own the reliance on a specific cloud region, or the dependence on a vendor. Otherwise, after a failure, the blame floats around the office like a helium balloon. Everyone points at it, but nobody grabs the string.

Best regards,

George Lekatis

George Lekatis
President of the IARCP

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

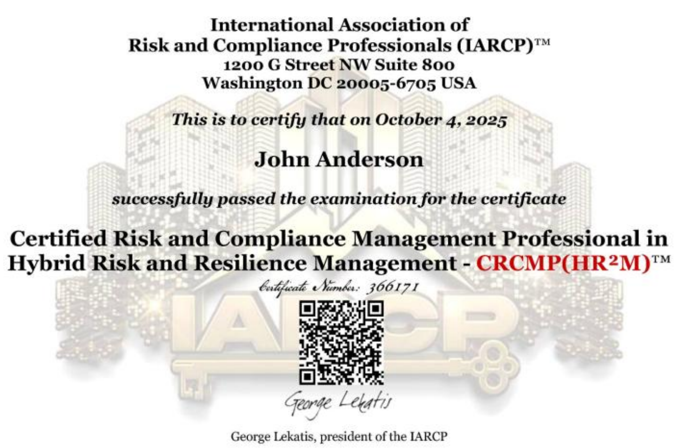
We are thrilled to announce the launch of the Certified Risk and Compliance Management Professional in Hybrid Risk and Resilience Management - CRCMP(HR²M), online training and certification program.

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

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

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

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



Number 1 (Page 6)

Preserving the dynamism and credibility of stress testing
Michael S Barr, Member of the Board of Governors of the Federal Reserve System, at the Peterson Institute for International Economics, Washington DC

Number 2 (Page 8)

ECB presents findings from digital euro innovation platform and announces second round of experimentation

Number 3 (Page 12)

PRA proposes reduced reporting requirements for banks
The Prudential Regulation Authority (PRA) has today announced proposals to reduce regulatory requirements for banks by deleting 37 individual reporting templates.

Number 4 (Page 14)

The "Custodians of Audit Knowledge": The Need for Academic Research and The Longstanding Relationship Between the PCAOB and the Academic Community
George R. Botic, PCAOB Acting Chair

Number 5 (Page 19)

Revisiting an interesting development missed by many during the summer.
Android Droppers: The Silent Gatekeepers of Malware

Number 6 (Page 20)

BKA und Nachrichtendienste warnen vor Anwerbeversuchen für Spionage und Sabotage über Soziale Medien

It is in German, can be easily translated

Number 7 (Page 22)

Cybersecurity Awareness Month

Number 8 (Page 26)

NIST SPECIAL PUBLICATION 1800-37

Addressing Visibility Challenges with TLS 1.3 within the Enterprise

Number 9 (Page 29)

Scientists unravel the atomic secrets of alpha plutonium

Covalent bonding in α-Pu is confirmed for the first time, offering new insights into its unusual properties

Number 10 (Page 33)

Space-based nuclear detonation detection mission endures

Number 1

Preserving the dynamism and credibility of stress testing

Michael S Barr, Member of the Board of Governors of the Federal Reserve System, at the Peterson Institute for International Economics, Washington DC

Today, I would like to discuss a vital tool for supervising the safety and soundness of the largest banks and preserving the stability of our financial system.

I was there, at the Treasury Department in 2009, when stress testing was first used in the United States in the heat of battle, an ad hoc measure to reverse a loss of confidence in U.S. banks that was a major force then driving the Great Recession.

By examining how the balance sheets of banks would be affected by a worsening of financial and economic conditions, this process was intended to reveal weaknesses that could threaten the solvency of banks and prevent them from playing their central role in the economy.

Stress testing ultimately succeeded in helping to restore confidence during the crisis, and in the aftermath this battle-tested tool became a formal and integral part of the effort to repair the ensuing damage and strengthen the banking system.

Stress testing has continued to evolve in the years since then to maintain that strength and help limit the chances of another devastating financial crisis. Stress testing changed as its purpose changed from wartime to peacetime—from mitigating the crisis to preserving safety, soundness, and stability.

It has changed as banks and regulators learned more about how stress testing works in practice and as part of an otherwise evolving supervisory and regulatory framework for banks that must necessarily adjust as finance itself evolves.

Adjusting regulation in this dynamic environment is challenging, and one of those challenges is dealing with unintended consequences.

The Federal Reserve made changes to stress testing in 2020 intended to make it more predictable and to better integrate it with overall capital regulation, but those changes are now at the center of litigation brought by large banks.

The Fed responded in April by proposing more changes intended to address these criticisms. But as I explained in voting against those measures, I believe these steps will substantially impair stress testing, concealing rather than revealing crucial weaknesses in the risk management of individual banks and in the stability of the financial system.

As the Federal Reserve Board considers these changes, I believe we should focus on how best to address the original purpose—and preserve the effectiveness—of stress testing.

As I will explain, I believe that the best way to further these goals is to separate stress testing from capital requirements in order to maximize the informative value of the tests and their results and untangle them from the larger and complex task of setting capital requirements.

I will lay out that alternative approach toward the end of these remarks, but first I believe it is helpful to take a step back and recall how stress testing has evolved to this point, then turn to where it should go from here.

It all began during the Global Financial Crisis. Capital markets froze, resulting in business failures and prompting the need for unprecedented public-sector intervention. Credit to households and businesses slowed to a trickle, and millions of people were losing homes and jobs. By the fall of 2008, there was a broad-based lack of confidence in the banking system, as large banks faced questions about their exposures to losses related to real estate and other assets.

These were questions that large banks in many cases couldn't credibly answer because of the complexity and opacity of their direct and indirect exposures to mortgages at the center of the crisis. Without this information, investors assumed the worst, driving down equity prices of banks, which complicated efforts by banks to bolster their balance sheets. Restoring confidence in the banking system required credible information from a reliable source.

Treasury worked with the Federal Reserve to design the Supervisory Capital Assessment Program (SCAP) to test the capital adequacy of what were determined to be the 19 most systemically important banking and financial institutions.

In addition, Congress had provided a backstop in the form of the Troubled Asset Relief Program (TARP), the Federal Deposit Insurance Corporation (FDIC) had backstopped bank funding through guarantees, and the Federal Reserve had stepped up in significant ways to bolster the financial system and the economy.

The existence of a government backstop played a big role in the success of the first stress test. With the use of public funding on the line, the rigor and transparency of the stress test was doubly important.

To read more:
https://www.federalreserve.gov/newsevents/speech/barr20250925a.htm

Number 2

ECB presents findings from digital euro innovation platform and announces second round of experimentation

EUROPEAN CENTRAL BANK | EUROSYSTEM

- Experimentation with almost 70 market participants highlights digital euro's potential to foster innovation and financial inclusion

- ECB to launch second round of experimentation through platform next year to maximise innovation potential

- Conditional payments identified as possible key driver of innovation for consumers and businesses

A digital euro could foster innovation in the European payments system and boost financial inclusion, according to a report published today on the outcome of the first iteration of the digital euro innovation platform – an initiative launched by the European Central Bank (ECB) in October 2024 for collaboration and experimentation with digital euro project stakeholders.

This iteration of the innovation platform brought together almost 70 market participants, including merchants, fintech companies, start-ups, academia, banks and other payment service providers, to explore possible applications of the digital euro.

Participants joined one or both of two workstreams: "visionaries" and "pioneers". The visionaries focused on gathering innovative ideas and exploring the long-term potential of the digital euro, while the pioneers concentrated on technical experimentation. Both workstreams highlighted the importance of harmonised standards, a shared infrastructure and ongoing collaboration with market participants for ensuring the scalability, reliability and usability of the digital euro across the euro area.

Today's report presents the findings of the two workstreams. It describes the innovations and applications that the digital euro platform could enable, some of which are highlighted below.

Conditional payments, i.e. payments that are triggered automatically when predefined conditions are met, were identified as a possible key driver of innovation and an example of how the digital euro could improve the day-to-day lives of European citizens.

As set out in the current draft legislation, a digital euro would offer core technical capabilities, such as the reservation of funds functionality, which would allow money to be set aside while a payment in progress. Unique features such as this, in conjunction with the harmonised standards established by the digital euro rulebook, would allow payment service providers to develop the additional technical layer needed to enable conditional payments.

In online shopping transactions, for example, funds could be released to the seller only after the buyer confirms that the item has been delivered, ensuring greater consumer protection. Insurance reimbursements could be automated and, in the case of delayed services, refunds could be streamlined.

For shared mobility services and public transport, conditional payments could enable tap-and-go transactions and automatically calculate the best available fare. These concepts were successfully tested in a simulated digital euro environment.

Conditional payments were also tested in the context of business-to-business (B2B) payments, which typically involve larger amounts and more complex contractual agreements. It was found that a digital euro would contribute to reducing fragmentation and costs for B2B payments, while bringing increased standardisation and liquidity.

Integrated electronic receipts (e-receipts) within the digital euro ecosystem could provide consumers with structured access to their purchase records, simplifying tasks such as returns, warranty claims, expense reporting and personal budgeting.

For merchants, e-receipts could significantly reduce operational costs and improve efficiency. Eliminating billions of printed receipts each year would not only simplify people's lives, but also bring clear environmental benefits such as reducing chemical waste, resource use and emissions. E-receipts would be strongly encrypted, meaning they could only be seen by the buyer and the seller.

The digital euro could also improve inclusion and accessibility, for example with tailored wallets for children to help them learn how to spend and save responsibly from a young age. Students could gain easier access to dedicated benefits and discounts with free digital euro wallets.

To ensure accessibility, the digital euro interface could incorporate user-friendly features such as voice-controlled transactions, large-font displays, and guided onboarding processes.

Following the success of these partnerships and amid further demand from market participants, the ECB has decided to launch a second round of experimentation in order to maximise the digital euro's potential for innovation. More details will be announced during the first half of 2026.

"We asked market participants to imagine the many opportunities a digital euro could offer consumers and merchants. Their enthusiastic response shows the immense scope for the digital euro to play a transformative role in the European payments landscape," said ECB Executive Board member Piero Cipollone at Bocconi University in Milan, where the report was presented on Friday at a payments conference attended by several innovation platform participants. "By fostering collaboration and providing a harmonised infrastructure, the digital euro can enhance the payment experience for Europeans, while enabling market participants to develop innovative services and business models."

The digital euro's extensive reach would ensure that these innovative ideas are instantly accessible to all consumers and merchants in the euro area, addressing the limitations typically associated with the closed ecosystems of other payment methods.

The ideas explored as part of the innovation platform initiative are still at the experimental stage. The Eurosystem will continue engaging with stakeholders to ensure that the digital euro's design meets the needs of future users and the market.

Figure 4
Conditional payment

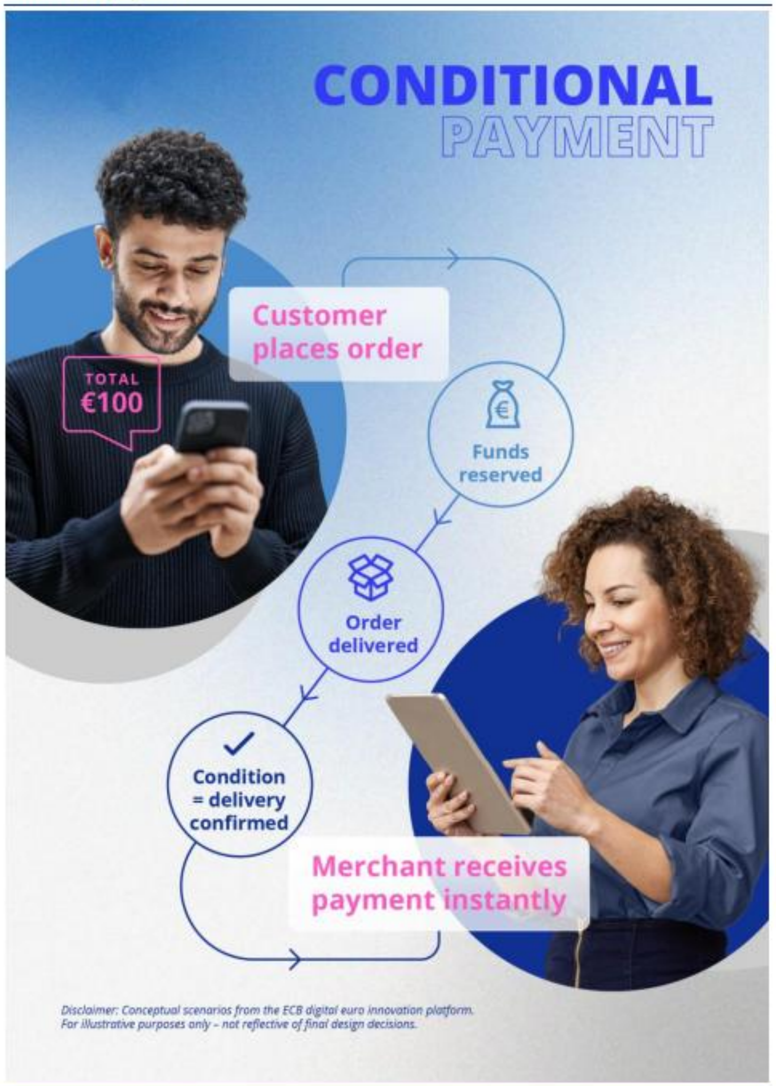


Figure 5
Tap & Go functionality

EUROPEAN CENTRAL BANK
EUROSYSTEM

Digital euro innovation platform

Outcome report: pioneers and visionaries workstreams

To read more:
https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.deprep250926_innovationplatform.en.pdf

Number 3

PRA proposes reduced reporting requirements for banks
The Prudential Regulation Authority (PRA) has today announced proposals to reduce regulatory requirements for banks by deleting 37 individual reporting templates.

Bank of England

The Prudential Regulation Authority (PRA) announced proposals to reduce regulatory requirements for banks by deleting 37 individual reporting templates.

The proposals represent an initial set of targeted deletions of whole reporting templates that were inherited from European Union regulations. This is a first deliverable from the PRA's strategic review of its banking data collections – the Future Banking Data project.

The vast majority of the templates being removed relate to financial reporting, improving an area which has been previously identified by firms as having overlapping and complex requirements.

The PRA has decided that these templates cover data which are either no longer necessary to support its work or are already available elsewhere. Their removal should benefit firms by reducing their administrative costs.

Rebecca Jackson, Executive Director for Authorisations, Regulatory Technology, and International Supervision and executive sponsor of Future Banking Data, said: "It's essential to get the right data from firms in order to supervise them properly. But it's also important that we do that as efficiently as possible and in a low-cost way, so they can focus on their core business and supporting their customers. Today's announcement is another example of our ongoing work to enhance the proportionality of our regulation and support growth without risking the stability of firms or the wider financial system."

The proposals build on a raft of simplifications the PRA has already made to reporting for insurers, reducing insurance reporting by one third. Firms are already benefitting from those changes.

This consultation will run for one month, with the goal of implementing the changes on 1 January 2026. This would save the industry an estimated £26 million annually.

The consultation forms an initial phase of the PRA's Future Banking Data initiative, which aims over time to significantly reduce burdens on firms whilst ensuring the PRA receives the high-quality data it needs to do its job.

The proposed changes, and the planned future work in this area, build upon other recent announcements by the PRA designed to support growth. These include options to enhance competition in the mortgage market, work to make the resolution regime more proportionate, and plans to simplify the capital regime for smaller, UK-focused banks.

The Bank's Statistical Reporting team have launched a consultation to discontinue the collection and publication of Form BN on the further sectoral breakdown of non-resident monetary financial institutions.

To read more:
https://www.bankofengland.co.uk/news/2025/september/pra-proposes-reduced-reporting-requirements-for-banks

Number 4

The "Custodians of Audit Knowledge": The Need for Academic Research and The Longstanding Relationship Between the PCAOB and the Academic Community
George R. Botic, PCAOB Acting Chair

Good afternoon. Thank you, Josh [White], for the kind introduction, and my heartfelt thanks to the entire Office of Economic and Risk Analysis (OERA) for the incredible work that makes this conference possible. Without you, we would not be here.

I want to extend a warm welcome to all of you, today's participants, for being here and presenting your ideas, and I also want to acknowledge the editors at Management Science for partnering with OERA on this event—thank you. Your collaboration elevates our shared mission of rigorous academic research that will assist us with our audit oversight activities and investor protection mission.

Before I continue, please know that my remarks this afternoon are provided in my official capacity 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.

I understand that there are several students in the audience today. It is wonderful you made time to join us, and your thoughts and ideas are equally important and welcome in our discussions.

Speaking to students pursuing careers in accounting and auditing is, personally, one of the most meaningful parts of being a Board Member.

So far this year, I have spoken to 13 student groups around the country with two more scheduled for next week.

Each of these conversations is a reminder that the future of financial integrity and public trust rests in the hands of curious, principled auditors who will not only uphold the standards of this noble profession but will elevate them.

The importance of financial statement auditing cannot be overstated. In fact, a former colleague referred to auditing as the "sport of kings", and after my interactions with students from across the country, I am pleased to report that the future of our profession—the future of the "sport of kings"—is in good hands.

But make no mistake, this is not by chance. It is the result of the dedication and commitment of the academic community and those who educate, mentor, and prepare students to enter the accounting profession. I want to thank you for all you do for the students.

When I was thinking about today's conference, I was reminded of Bernard Baruch—the successful financier, trusted advisor to seven U.S. presidents, and the namesake of Baruch College. He is largely attributed to saying, "Millions saw the apple fall, but Newton was the one who asked why."

I tell this story because today I am in front of the very people who ask why. Academics do not just record the fall; they analyze the forces at play—identifying where auditors succeed, where they stumble, and where the next blind spot might emerge.

During my time, I want to explore the following three topics: first, the longstanding relationship between the PCAOB and the academic community; second, why rigorous scholarly research matters to our work; and third, how we can deepen our partnership going forward.

The Long-Standing Relationship Between the PCAOB and the Academic Community

The PCAOB's collaboration with the academic community began during our earliest days—with the establishment of the PCAOB's own in-house research office in 2004—just one year after the organization was officially formed.

Twenty-two years ago, I was an inspector when the organization was just getting off the ground. At that time, the impetus for establishing what was then called the Office of Financial Analysis and Risk Assessment was to have an established division of accountants, analysts, and economists within the PCAOB to provide the Board with advice and expertise on financial reporting trends and economic analysis.

More than two decades later, that sentiment remains the same, and we have been fortunate to recruit an incredible cohort of established, respected, and revered financial academics to the PCAOB over the years, from Doug Carmichael and Gary Holstrum, to Luigi Zingales, Christian Leuz, and Martin Schmalz, to name but a few.

I would be remiss not to add our current team within OERA to that list. These are renowned scholars who are frequently invited to speak at conferences all over the world to present their findings and share their insights. I am grateful to count them as my colleagues at the PCAOB.

At the same time, the PCAOB is no stranger to hosting its own conferences. The first PCAOB academic conference took place in 2004. A decade later, the Conference on Auditing and Capital Markets was launched. This year's conference will be held on October 16 and 17 in Washington, D.C. Please consider joining us if you have not already.

While today's event, OERA's Registered Reports Conference, is a newer venture, the momentum behind it is growing. Last year's Registered Reports Conference generated such enthusiasm that we received more than one hundred proposals in advance of this year's conference, which the team in OERA and the editors of Management Science had the incredibly difficult task of whittling those down to the nine submissions on the agenda today.

Earlier, we heard from the editors of Management Science about the PCAOB's impact as an effective regulator. Academics lending their time and expertise to help inform our work hearkens back to the synthesis projects conducted in the early years of the PCAOB.

The first was conducted from 2005 to 2008 and resulted in 10 research synthesis papers. The second project was from 2011 to 2015 and resulted in 13 papers. These efforts have greatly benefited our standard setting projects.

The PCAOB's advisory groups have long benefited from the perspectives of numerous academic participants over the years2 including several who authored papers being presented today: Colleen Honigsberg and Shiva Rajgopal, both Standards and Emerging Issues Advisory Group (SEIAG) members, and Nemit Shroff, an Investor Advisory Group (IAG) member. We will also hear from Robert Knechel, a former SEIAG member, who will be a discussant later today.

The PCAOB's Economic Research Fellowship program brings academic economists to the PCAOB for a year, during which they work with PCAOB staff on projects and pursue a Board-approved research proposal. We have now seen 18 PCAOB fellows come and go through our doors, and they have authored 13 published papers and 12 additional working papers.

For example, these scholars have examined topics such as how the allocation of audit hours shapes audit quality, the consequences of small and midsized firm mergers on public company audit market competition, and the association between auditors' use of in-house specialists and audit quality.

They have quantified the link between waived audit adjustments and the audit process, studied how partner industry expertise and mandatory partner rotation affect audit outcomes, and explored how firms' use of shared service centers and quality control systems influence audit quality and fees.

Over the years, this work has influenced and informed the PCAOB's decision making including in our inspection program and standard setting and rule-making activities.

Why Research Matters to the PCAOB

Which brings me to the second topic: why research matters to the PCAOB.

Let me start by exploring how research improves decisions. When we draft or update auditing standards, we make choices that come with real costs and benefits. Evidence from scholarly research informs those choices. We need to understand how auditors perform key tasks, how public companies respond to those audit tasks, how investors interpret and use disclosures, and how the structure of the audit market shapes incentives.

Academic findings help inform auditing standards by providing conceptual and empirical support to compare the expected costs and benefits of the standards. If you look at our economic analyses, you will see that OERA staff carefully and comprehensively review the academic literature and its findings.

For example, in our release adopting AS 1000, the economic analysis carefully considered the academic literature related to professional skepticism and how it relates to PCAOB standards.

After we adopt auditing standards, your research helps us in our post-implementation review analysis to evaluate whether expected costs and benefits materialize and deepen our understanding of a standard's impact on audits of public companies and broker-dealers. Research also provides insights into unintended consequences, both positive and negative.

Next, speaking more broadly, is how research improves our oversight activities.

Academic work helps assess the impact of the PCAOB's inspection program. For example, scholarly research studies on how PCAOB inspection access to non U.S. auditors are associated with audit quality, and whether initial international inspections improve the audit quality for those auditors' other engagements. That work informs us when we plan and communicate inspections across jurisdictions.

The overarching point I want to make today is that research improves our foresight by anticipating changes in the audit profession itself. For example, how private equity investment, ownership structure, and firms' financing models are being reshaped and reconsidered, and how ongoing firm consolidations can affect competition and choice and potentially audit quality.

Another emerging trend to consider is how technology is changing how audit work is performed. There is growing evidence that investors and analysts are using AI tools to interpret financial information as they make investment decisions. These tools offer the possibility of synthesizing information from Form 10-Ks, Form 10-Qs, earnings releases, and transcripts of earnings calls.

Yet, a July report from Goldman Sachs analysts pointed out that "the vast majority of [U.S.] companies have not incorporated AI into regular workflows".

So, while the research appears to show that AI has yet to be fully adapted by companies, there is no question that technology is evolving and advancing every single day, and we all need to be able to adapt and shift along with it.

Advancing The PCAOB's Partnership with the Academic Community

This calls to mind Professor Eldar Maksymov's recent paper on audit academia at a crossroads.

He wrote that as “the custodians of audit knowledge”, audit academics find themselves at a fork in the road as it pertains to AI: “Our role is not to mirror the profession’s present, but to help define its future.” He continued, “It is an invitation to join forces with practitioners and regulators to revitalize our shared mission: Strengthening capital markets through timely, high-quality assurance and insight that serves the public interest.”

Professor Maksymov’s sentiments that engagement of academics, practitioners, regulators, and I would include investors, to join forces could not be better stated.

We need rigorous academic research on these topics, including evidence that shows not only how and whether emerging issues from private equity investments in accounting firms to AI impact audit quality, but also where they may introduce new risks and new opportunities.

The academic community’s generous expertise helps the PCAOB to understand how broader economic and technological forces may impact audits and audit quality - and ultimately - how investors are affected.

As I conclude, I encourage you to continue collaborating with the PCAOB and providing your work, your ideas, and your feedback. Share your early-stage research as well as your peer-reviewed research. Participate in our conferences. Submit your proposals. Recommend colleagues to become PCAOB fellows or apply to become one yourself. And most importantly, continue asking the tough questions.

Let us go back to Mr. Baruch, millions may watch the apple fall, but those who ask why unlock and discover the deeper truths.

It is these truths that academics, “the custodians of audit knowledge”, dedicate their careers to pursuing. And it is these truths that we at the PCAOB need to hear and learn from in order to continue fulfilling our mission to protect investors.

Thank you for your dedication and commitment to scholarly research and your students. I look forward to learning more from you and to continuing our partnership.

I welcome your questions and any comments you may have.

To read more:
https://pcaobus.org/news-events/speeches/speech-detail/the--custodians-of-audit-knowledge---the-need-for-academic-research-and-the-longstanding-relationship-between-the-pcaob-and-the-academic-community

Number 5

Revisiting an interesting development missed by many during the summer.
Android Droppers: The Silent Gatekeepers of Malware

"In recent months, we at ThreatFabric have observed a clear shift. Alongside banking trojans, droppers were also used in campaigns delivering relatively “simple” malware such as SMS stealers and basic spyware, often disguised as government or banking apps in India and other parts of Asia."

To read more:
https://www.threatfabric.com/blogs/android-droppers-the-silent-gatekeepers-of-malware

Number 6

BKA und Nachrichtendienste warnen vor Anwerbeversuchen für Spionage und Sabotage über Soziale Medien

It is in German, can be easily translated

Attempts to recruit individuals for sabotage and espionage activities are increasingly being carried out via social media.

The Federal Criminal Police Office (Bundeskriminalamt, BKA), the Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz, BfV), the Federal Office of Military Counterintelligence (Bundesamt für den Militärischen Abschirmdienst, BAMAD), and the Federal Intelligence Service (Bundesnachrichtendienst, BND) have observed a rise in espionage and sabotage activities in Germany and other countries.

The perpetrators are believed to be intelligence services, which use social media themselves or through intermediaries to recruit people for espionage and sabotage in or against Germany.

The individuals recruited in this way are referred to as “low-level agents” or “disposable agents.” They commit criminal acts in Germany without having received any intelligence training — sometimes in exchange for small payments and often without knowing who their true principals are or what purpose their actions serve.

Anyone who engages in such contacts or activities risks becoming involved in intelligence operations such as espionage or sabotage and being prosecuted under criminal law.

The security authorities point out in this context that engaging in agent activities for sabotage purposes and intelligence-related agent activities are criminal offenses that, in particularly serious cases, can be punished with up to ten years of imprisonment.

Several suspected cases are currently under investigation in Germany, including arson, property damage, drone flights, as well as suspicious photography and video recording.

These offenses are directed against critical infrastructure facilities in the energy, transport and traffic, logistics, information and communication technology sectors, as well as against military installations and the defense industry.

To raise awareness of this relatively new form of recruitment, the Federal Criminal Police Office (BKA), together with the Federal Office for the Protection of the Constitution (BfV), the Federal Office of Military Counterintelligence

(BAMAD), and the Federal Intelligence Service (BND), has developed the campaign “Don’t Become a Disposable Agent!”.

The campaign explains this phenomenon and aims to sensitize the wider public to the issue. Its goal is to ensure that social media users do not respond to recruitment attempts and instead report them to the security authorities.

(Disposable Agents: Short Mission, High Risk)

To read more:
https://www.bnd.bund.de/SharedDocs/Downloads/DE/Pressemitteilungen/250902_pressemitteilung_LLA.pdf?__blob=publicationFile&v=3

https://www.bka.de/DE/Landingpages/LLA/lla_node.html

Number 7

Cybersecurity Awareness Month

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

October is Cybersecurity Awareness Month!

For more than 20 years we have spotlighted the importance of taking daily action to reduce risks when online and using connected devices. This year, we focus on the government entities and small and medium businesses that are vital to protecting the systems and services that sustain us every day and make America a great place to live and do business: the nation's critical infrastructure.

Much of the nation's critical infrastructure is owned and operated by state, local, tribal, and territorial governments as well as private companies. Additionally, vendors, suppliers, and other parts of the supply chain that support or are connected to critical infrastructure play a critical cybersecurity role.

This year's theme is Building a Cyber Strong America, highlighting the need to strengthen the country's infrastructure against cyber threats, ensuring resilience and security.

Cyber threats don't take time off. As the federal lead for Cybersecurity Awareness Month and the nation's cyber defense agency, the Cybersecurity and Infrastructure Security Agency, or CISA, urges all U.S. small and medium businesses and state, local, tribal, and territorial governments to take one action today to improve their cybersecurity.

Secure Your Business

Critical infrastructure relies on small and medium business to supply, support, or even operate services we all rely on. Make sure your business is cyber secure so you don't experience an incident that could impact critical services.

You Can Protect Your Business from Online Threats

Your business is digitally connected—to employees, vendors and customers—and it has valuable data that cybercriminals want. No business is too small to be a target. From ransomware to phishing, cyber threats are growing.

In 2024, the FBI reported over $2.7 billion in losses from business email compromise alone, just one of many threats businesses face.

Small and mid-sized businesses are especially vulnerable because they may not have as many resources to dedicate to cybersecurity.

Securing Critical Infrastructure

Businesses directly and indirectly involved with critical infrastructure, including manufacturers, vendors in the supply chain and utility suppliers, are particularly at risk.

Threat actors actively look for open vulnerabilities, like weak credentials or outdated software, to break into business systems and plan a wide-ranging attack.

Often they look for access to critical infrastructure to hold systems for ransom, which leads to a disruption of supply. Don't let a weak link in your business lead to problems. Learn important (and achievable) ways you can protect your business and community.

CISA recommends that businesses at all levels implement eight cybersecurity best practices and offers no-cost information, services and tools to help you get started.

Start Here: Four Essentials to Protect Your Business

Cybercriminals look for easy targets. Businesses without basic precautions are vulnerable. Start with these four essential steps to safeguard your data and enable your employees to stop attacks before they happen.

- Teach Employees to Avoid Phishing: Phishing tricks employees into opening malicious attachments or sharing sensitive information. Train staff to recognize and report suspicious activity.

- Require Strong Passwords: Strong passwords are a simple but powerful way to block criminals from accessing your accounts through guessing or automated attacks. Make them mandatory for all users.

- Require Multifactor Authentication (MFA): MFA—also known as 2-factor authentication—adds an extra layer of security beyond passwords. Require it to make accounts significantly more secure. Use phishing resistant MFA where available.

- Update Business Software: Outdated software can contain exploitable flaws. Promptly install security updates and patches to keep your systems protected.

Next Step: Level Up Your Defenses

With the four essentials as your foundation, level up by implementing three additional practices.

- Use Logging on Business Systems: Log activity so your team can monitor signs that threat actors may be trying to access your systems. Learn how to monitor key information to protect your business.

- Back Up Business Data: Incidents happen, but when you back up critical information, recovery is faster and less stressful. Put a backup plan in place that aligns with your organization's recovery point objective to protect your systems and keep things running smoothly.

- Encrypt Business Data: Encrypting your data and devices strengthens your defense against attacks. Even if criminals gain access to your files, information stays locked and unreadable. Make encryption part of your security strategy.

An Additional Step You Can Take

- Report Cyber Incident Information to CISA: When organizations and CISA share threat information, everyone is more secure. Report incidents to help CISA warn others and get information in return to help you stay ahead of threats.

Create a Culture of Cybersecurity

As a business leader, your commitment to cyber readiness sets the tone for your entire organization. Implementing our seven cybersecurity best practices will make your organization so much more secure from threats. In addition, create a culture of cybersecurity to enforce stronger policies and set your team up for success.

- Start by empowering your IT and security leaders. Define IT leadership roles within your organization early. Include them in high-level decisions that affect risk and operations, and make it clear across your organization that cybersecurity is a company priority. Security leaders should have the authority and support to act quickly during an attack.

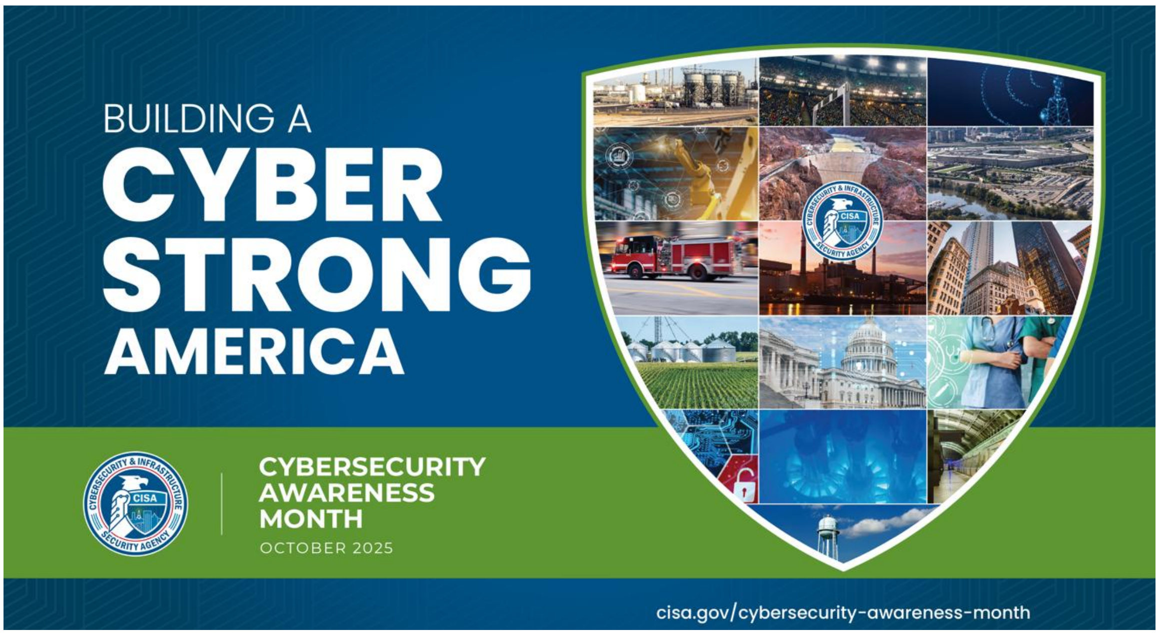
- Share your cybersecurity policies and procedures with your employees. Make training a regular part of staff onboarding and ongoing development. Plan engaging cybersecurity training activities. Evaluate the effectiveness of security trainings through decrease or increase of security incidents and reporting during phishing simulations. Explore our no-cost resources, including a printable cybersecurity BINGO card for organizations that encourages learning while building a shared sense of responsibility.

- Create an Incident Response Plan.Involve your leadership team in regular tests of the response plan and walk through how your company would respond if systems went down, data was stolen or your networks were compromised. Practicing now means less confusion and downtime later.

- Make cyber incident reporting part of your company culture. Set a low threshold for reporting suspicious activity. Even blocked attacks or strange system behavior should be flagged and, when appropriate, reported to government agencies like CISA.

- Focus on continuity. Identify your most critical systems and make sure they can stay up and running during a cyber incident. Have backups ready and test them regularly. If your business depends on industrial systems or specialized tech, ensure your team knows how to operate them manually if needed. Consider using CISA's no-cost SCuBA tool to harden software-as-a-service (SaaS) configurations to support best practices on cloud platforms. CISA also offers the Malcom tool at no-cost, which is an open-source tool for industrial control systems (ICS) that provides network analysis.

Cyber threats are a reality, but business disruption doesn't have to be. Build a culture of awareness, action and accountability.



To read more: https://www.cisa.gov/cybersecurity-awareness-month

Number 8

NIST SPECIAL PUBLICATION 1800-37
Addressing Visibility Challenges with TLS 1.3 within the Enterprise

There are sector specific requirements that call for organizations to monitor network activity, protect sensitive data, and demonstrate security controls.

Enterprises leverage network traffic visibility in their security operations centers to prevent, detect, and respond to cybersecurity threats.

Enterprises moving to newer network security protocol standards such as TLS 1.3 will face challenges for maintaining network traffic visibility.

Modern protocol designers have changed protocols to strengthen security properties that protect the secrecy of historical network traffic.

This is possible even if the servers' long-term secret keys are compromised—a property known as forward secrecy.

However, forward secrecy has created significant challenges for the network visibility strategies used by enterprises.

The National Cybersecurity Center of Excellence (NCCoE), in collaboration with technology providers and enterprise customers, initiated a project demonstrating options for maintaining visibility within an enterprise adopting these new security protocols.

The demonstrations are suitable for voluntary adoption across a wide range of enterprise architectures.

They are scalable, actionable, and application protocol-agnostic, as well as usable in real-time following post-packet capture.

Enterprises using the Transport Layer Security (TLS) 1.2 protocol without forward secrecy deploy tools and architectural solutions that provide visibility into enterprise traffic within their network.

Enterprises have regulatory and compliance requirements to maintain visibility into received network traffic to enable the organization's security monitoring, analysis, and management policies.

An enterprise will not be able to use its deployed tools and architectural solutions that provide visibility into enterprise TLS 1.2 traffic to have visibility into TLS 1.3 traffic.
This publication includes demonstrated approaches for enterprises to adopt TLS 1.3 to allow enterprises to benefit from the security functionality of TLS 1.3 while maintaining the visibility into received network traffic.

This publication describes the motivation, approach, architecture, build implementation, demonstration scenarios, results, and risk and compliance management characteristics for the demonstrated proofs of concept.

The top-level overview provides links to technical details that are contained in online NIST pages.

The linked files provide detailed technical information for each demonstration that TLS visibility implementers can adopt in their own environments.

The demonstrations in this publication to maintain visibility are not intended as a recommended default or even for common use but to assist in those areas where, as OMB M 22-09 states: "…as agencies segment their networks, move away from intranets, and permit access to enterprise services from any network, inspecting traffic in these environments will become less practical and less valuable over time. In other places, deep traffic inspection may be more valuable and can create less of an increase in attack surface."

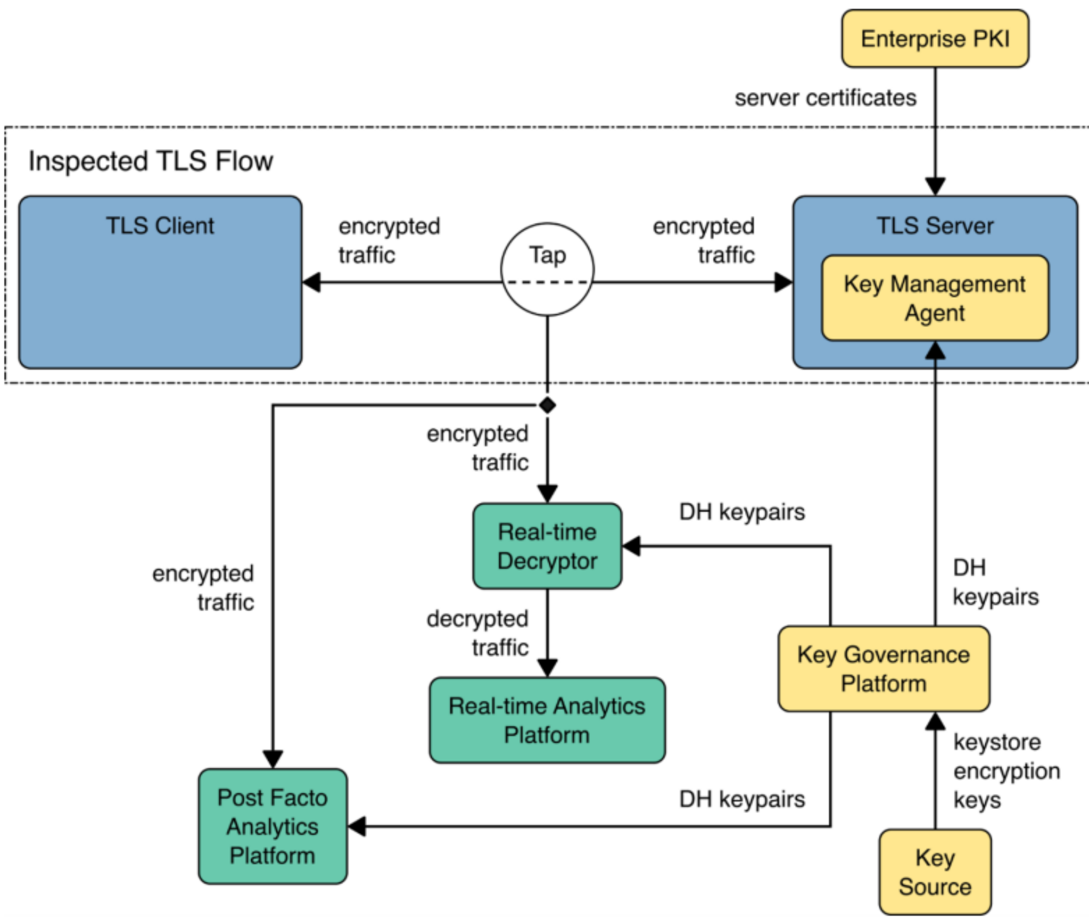


Figure 4-1 Middlebox (Break and Inspect) Functional Architecture

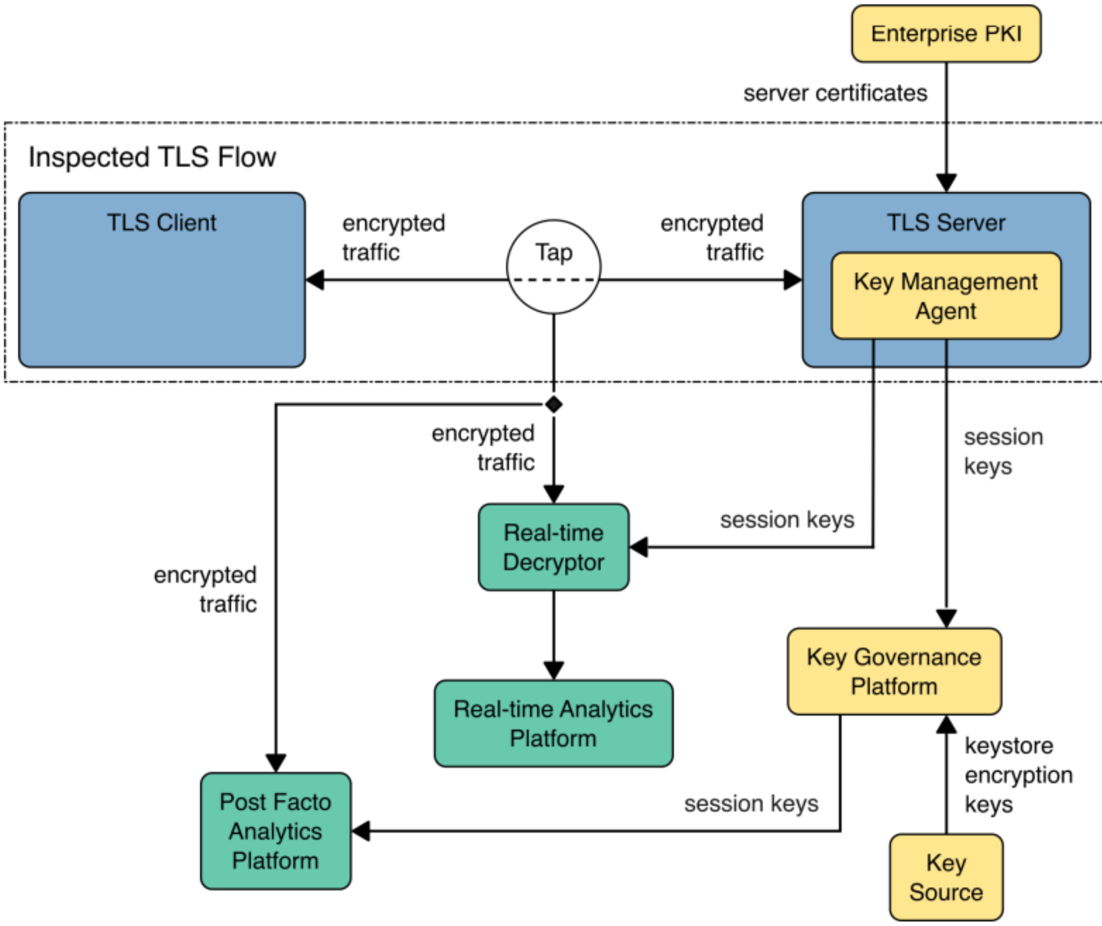


Figure 4-2 Passive Inspection - Exported Session Key Functional Architecture

To read more:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-37.pdf

Number 9

Scientists unravel the atomic secrets of alpha plutonium

Covalent bonding in α-Pu is confirmed for the first time, offering new insights into its unusual properties

This story was written and first published by Brookhaven National Laboratory. This research was supported in part by the Laboratory Directed Research and Development program at Los Alamos National Laboratory and uses resources provided by the Los Alamos National Laboratory Institutional Computing program; use of the National Synchrotron Light Source-11 at Brookhaven is supported by the U.S. Department of Energy.

Plutonium has captured the attention of scientists since its discovery in the early 1940s. This enigmatic element has an important role to play in emerging energy technologies like nuclear batteries and reactors, but it also has complicated electronic behavior that causes some intriguing effects. Its electron structure contributes to unconventional entropic properties at low temperatures, multiple phase transitions before melting and complex bonding patterns.

A History of Plutonium:
https://www.lanl.gov/media/publications/actinide-research-quarterly/0922-shining-light-on-a-dark-element

LANL Home / Media / Publications / Actinide Research Quarterly /

September 21, 2022

A History of Plutonium

Shining Light on a Dark Element

Owen Summerscales, Editor

Although scientists are eager to explore these intriguing properties, studying plutonium remains notoriously difficult. Its strong electronic correlations, complex quantum effects like spin-orbit coupling, and changes due to radioactive decay make both experimental research and computer simulations challenging. To add further complexity, plutonium is also found in several different allotropes — forms of the same element with different atomic arrangements. Plutonium's alpha phase (α-Pu), for example, has a particularly complicated atomic structure. Understanding the complex bonding of this phase seemed like a worthwhile challenge for a newly formed collaboration of scientists to tackle.

Motivated by past theoretical work, a research team led by Los Alamos National Laboratory combined advanced computer simulations and high-precision X-ray measurements to more fully understand how atoms bond in α-Pu.

This led to the first-ever plutonium experiments at the National Synchrotron Light Source II, a DOE Office of Science user facility at DOE's Brookhaven National Laboratory. The team worked closely with Milinda Abeykoon, lead beamline scientist at the Pair Distribution Function beamline at NSLS-II.

Their research found a mix of bonding types, including evidence of covalent bonding, where atoms share electrons, which helps explain some of α-Pu's larger-scale mechanical properties. Their results were recently published in Advanced Functional Materials.

Updated techniques reveal new insights

Unlike the regular, highly symmetrical crystal structure of plutonium's delta phase (δ-Pu), which is more commonly studied, the α-phase has a lot more structural complexity. Its atomic arrangement is highly distorted and exhibits a wide range of atomic bonding distances. Early theories suggested that different strengths of chemical bonds might exist in α-Pu, while largely ruling out covalent bonding. But until now, no one has directly studied those bonds experimentally.

"In the field of plutonium, researchers are often interested in its mechanical properties for nuclear technology applications," said W. Adam Phelan, a nuclear materials scientist at Los Alamos and co-lead author of the work. "You rarely get this bottom-up, atomistic understanding in plutonium science." Again, he noted other results suggested there was little to no covalent bonding, but those results were at odds with the mechanical properties that we understand about this allotrope. "These insights explain why α-Pu has certain macroscale properties."

To investigate how atoms in α-Pu bond, the team used a technique called pair distribution function (PDF) analysis, which can reveal how atoms move together in a structure — an important behavior in complex or disordered materials. PDF measurements provide valuable information about the local atomic structure.

They combined this experimental study with density functional theory (DFT) calculations to validate their atomistic models. DFT helps scientists study the behavior of electrons at the atomic scale by using a simplified approach that focuses on electron density rather than tracking each electron individually. This enables researchers to model complex materials and chemical systems with practical accuracy and computational efficiency.

"α-Pu is a particularly tricky system to study. Its structure is complex, which generates a lot of information," said Alexander Muñoz, a computational physicist at Los Alamos and co-lead author of this work. “That can make large-scale trends difficult to discern. We really pushed DFT to its limits for this work.”

Before employing any of these novel experimental techniques, a lot of planning and protocol had to be implemented at NSLS-II. On top of the material challenges of studying plutonium, there are also some practical ones. An experiment like this takes months of preparation and the expertise of several specialized teams.

Plutonium, X-rays, and strict safety protocols

Plutonium is a rare and highly regulated material that is difficult to obtain. It’s also toxic, especially as a powder, and radioactive, demanding stringent safety measures.

To ensure the experiment was conducted safely and efficiently, experts from the Lab’s Radiological Control Division, NSLS-II’s management team, and the Environment, Safety, Health and Quality program provided critical oversight and support.

To start, there were strict limits on how much of the material could be brought on site to study, so the team was only able to work with a few precious milligrams. It’s not just the amount of plutonium in the experiment that’s monitored either. Brookhaven accounts for all special nuclear materials, which are regulated lab wide.

During preparation, those small samples were sealed in a custom-built triple containment system designed to ensure both radiological safety and X-ray transparency.

At the PDF beamline, the samples were mounted on translation stages to take measurements behind a lead-shielded hutch that was locked down during the entirety of the experiment. Panoramic cameras monitoring inside the hutch provided the team with real-time observation.

Once the experiment was ready to run, PDF’s flexible setup and high-energy range helped the team reach the answers they sought. Many recent updates and planned upgrades to the PDF beamline have made it the ideal tool for Phelan and his team to study this formidable material.

They were able to leverage the beamline’s high-energy capabilities to penetrate thick samples, and in future experiments, they can switch to another energy in minutes. For example, the beamline could accommodate the lower energy needed to perform small-angle X-ray scattering (SAXS) on a thinner plutonium sample.

The PDF analysis was combined with a computer-based modeling method called “reverse Monte Carlo.” These simulations helped the team identify patterns in the way atoms move together. They found that the atoms in α-Pu move in tightly linked groups, hinting at a significant amount of covalent bonding.

“The model captured the long-range structural order of the first dataset remarkably well,” Abeykoon said. “But the short-range atomic correlations revealed clear deviations from the expected pattern. That was exactly what we were expecting, though.”

Scientists used DFT calculations to further analyze the charge distribution and bonding structure, confirming their experimental observations. Their analyses revealed that α-Pu hosts a mix of bonding types: short bonds exhibit directional, covalent-like character, while longer bonds behave more metallically.

This mixed bonding landscape aligns with the theory that α-Pu’s structure is shaped by a Peierls distortion, when a material slightly changes the positions of its atoms to lower its overall energy. The presence of covalent bonding helps explain why α-Pu has been observed to behave more like a brittle solid than a malleable metal.

“We combined our approaches after a short conversation concerning some oddities I had noticed in the computed charge density,” Muñoz said. “Adam and I realized that we were discussing the same physics that was measured at NSLS-II.”

To read more: https://www.lanl.gov/media/news/0925-alpha-plutonium

Number 10

Space-based nuclear detonation detection mission endures

Roughly 12,550 miles above Earth, a constellation of U.S. global positioning satellites orbits the planet. GPS satellites also carry a sophisticated system designed to detect above ground nuclear detonations anytime, anywhere.

The Global Burst Detection system, developed by Sandia and Los Alamos national laboratories, carries a suite of sensors and instruments capable of identifying signals from nuclear detonations and providing real-time information to the U.S. military and government.

The final system in the current block of eight systems launched into space in May 2025. Meanwhile, the next series, scheduled for initial deployment in 2027, already has several units completed and ready to be integrated with host satellites.

This mission has endured for more than 60 years at the Labs. Teams of engineers, scientists and technologists work a decade ahead to develop new complex technologies that can withstand the harsh space environment while countering evolving threats.

"The launch of the final IIIA series Global Burst Detector marks an important milestone in our efforts to enhance nuclear detection capabilities," Sandia manager Andrew Stuart said. "The collaboration between Sandia National Laboratories and Los Alamos National Laboratory has been key to developing this advanced system, which will significantly contribute to our national security by improving our ability to detect nuclear detonations from space."

Marc Kippen, program manager for Space Systems and Science at Los Alamos, said, "The May launch is a testament to the decades of effort that it takes to maintain uninterrupted national security space capability. Los Alamos National Laboratory is proud to contribute to this important and enduring mission."

A space-based deterrent

The Global Burst Detection system serves as part of the space-based component of the U.S. Nuclear Detonation Detection System. This network of satellites, sensors and ground stations can detect, time-stamp and record electromagnetic pulse energy in specific bands, and X-ray and optical signals. This information helps the U.S. Air Force precisely determine the location, time and yield of a nuclear detonation.

Funded by NNSA, the sensors undergo rigorous testing and mission assurance processes to ensure they perform reliably during their 15-plus-year mission. Sandia performs a series of qualification tests, including shock, thermal, thermal vacuum, vibration and prompt X-ray tests, to demonstrate the system's ability to survive launch, deployment and operation in space. Sandia and Los Alamos design and produce the system's five subsystems, with Sandia integrating them into a complete detection system.

The final of the IIIA series

The last IIIA series Global Burst Detector launched into space from Cape Canaveral on May 30. Teams from Sandia, Los Alamos and the U.S. Space Force calibrated the system in June and conducted early on-orbit testing to verify functionality. For the final phase, the team will share the configuration and setting information with the U.S. Nuclear Detonation Detection System team for integration into the current satellite network.

Delivering the next generation

In 2024, Sandia and Los Alamos delivered the first two flight systems for the next generation of detectors, the IIIF, to Lockheed Martin for installation on GPS satellites. The first unit is scheduled to launch in 2027.

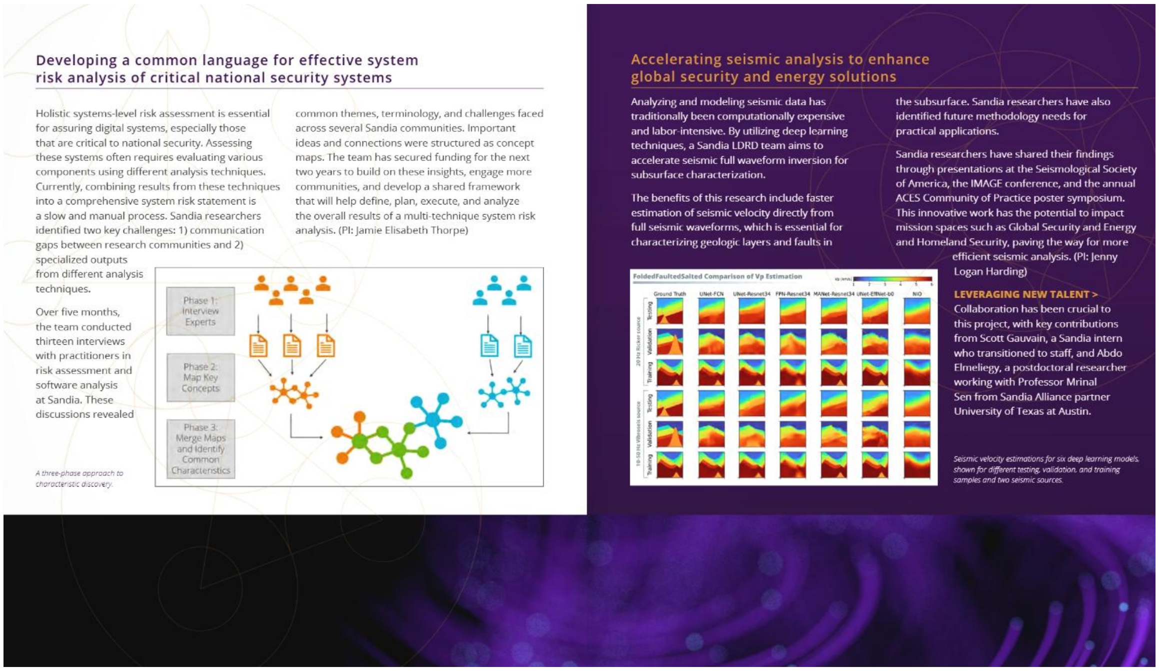
Teams from Sandia and Los Alamos worked together for 12 years to design and qualify the new system.

A key component of the IIIF series, the Spectral Imaging Geolocation Hyper-Temporal Sensor, or SIGHTS, has roots in Sandia's Laboratory Directed Research and Development program. More than a decade ago, researchers conducted basic science to push the boundaries of remote sensing. That work laid the foundation for a new megapixel-density optical sensor, capable of capturing tens of thousands of frames per second. This enables the sensor to better differentiate between legitimate signals and false positives.

Over the next decade, Sandia and Los Alamos plan to deliver, integrate and launch more IIIF Global Burst Detector systems to continue the mission.

To read more:
https://newsreleases.sandia.gov/space-based-nuclear-detonation-detection-mission-endures/

https://www.sandia.gov/research/flipbook/fy2024-ldrd-annual-report/#fy2024-ldrd-annual-report/1
(Note: Annual report, 111 pages)



Developing a common language for effective system risk analysis of critical national security systems

Holistic systems-level risk assessment is essential for assuring digital systems, especially those that are critical to national security. Assessing these systems often requires evaluating various components using different analysis techniques. Currently, combining results from these techniques into a comprehensive system risk statement is a slow and manual process. Sandia researchers identified two key challenges: 1) communication gaps between research communities and 2) specialized outputs from different analysis techniques.

Over five months, the team conducted thirteen interviews with practitioners in risk assessment and software analysis at Sandia. These discussions revealed common themes, terminology, and challenges faced across several Sandia communities. Important ideas and connections were structured as concept maps. The team has secured funding for the next two years to build on these insights, engage more communities, and develop a shared framework that will help define, plan, execute, and analyze the overall results of a multi-technique system risk analysis. (PI: Jamie Elisabeth Thorpe)

A three-phase approach to characteristic discovery.

Accelerating seismic analysis to enhance global security and energy solutions

Analyzing and modeling seismic data has traditionally been computationally expensive and labor-intensive. By utilizing deep learning techniques, a Sandia LDRD team aims to accelerate seismic full waveform inversion for subsurface characterization.

The benefits of this research include faster estimation of seismic velocity directly from full seismic waveforms, which is essential for characterizing geologic layers and faults in the subsurface. Sandia researchers have also identified future methodology needs for practical applications.

Sandia researchers have shared their findings through presentations at the Seismological Society of America, the IMAGE conference, and the annual ACES Community of Practice poster symposium. This innovative work has the potential to impact mission spaces such as Global Security and Energy and Homeland Security, paving the way for more efficient seismic analysis. (PI: Jenny Logan Harding)

LEVERAGING NEW TALENT >
Collaboration has been crucial to this project, with key contributions from Scott Gauvain, a Sandia intern who transitioned to staff, and Abdo Elmeliegy, a postdoctoral researcher working with Professor Mrinal Sen from Sandia Alliance partner University of Texas at Austin.

Seismic velocity estimations for six deep learning models, shown for different testing, validation, and training samples and two seismic sources.

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.

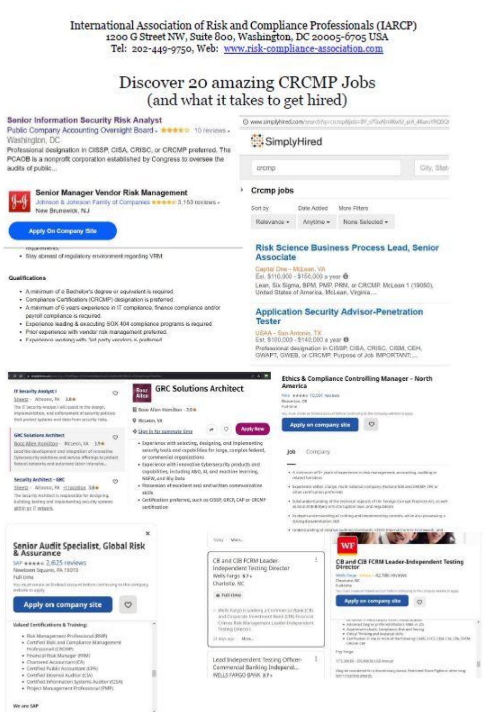
To learn more: https://www.risk-compliance-association.com/Privacy.htm

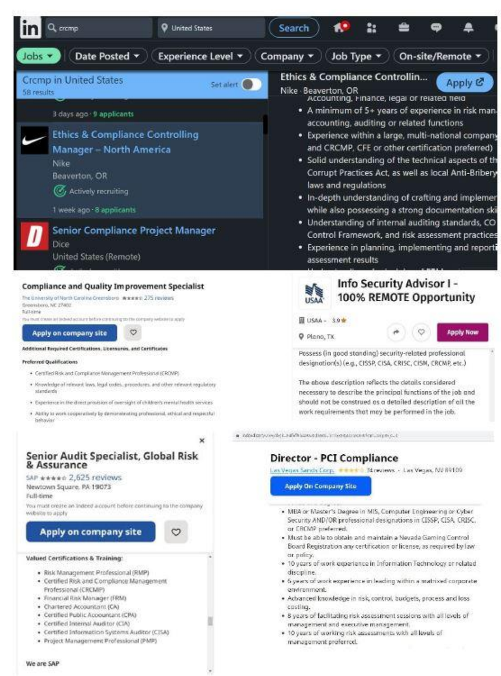
Our training and certification programs:

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:

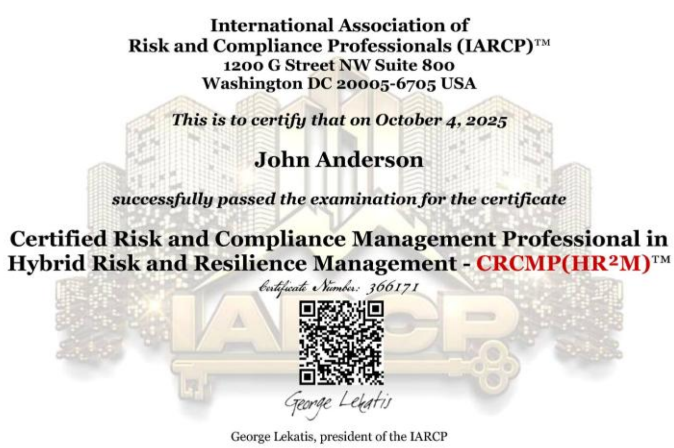
1. Moves from traditional risk and compliance frameworks into the management of multi-vector, cross-domain, and asymmetric threats that transcend conventional boundaries.

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

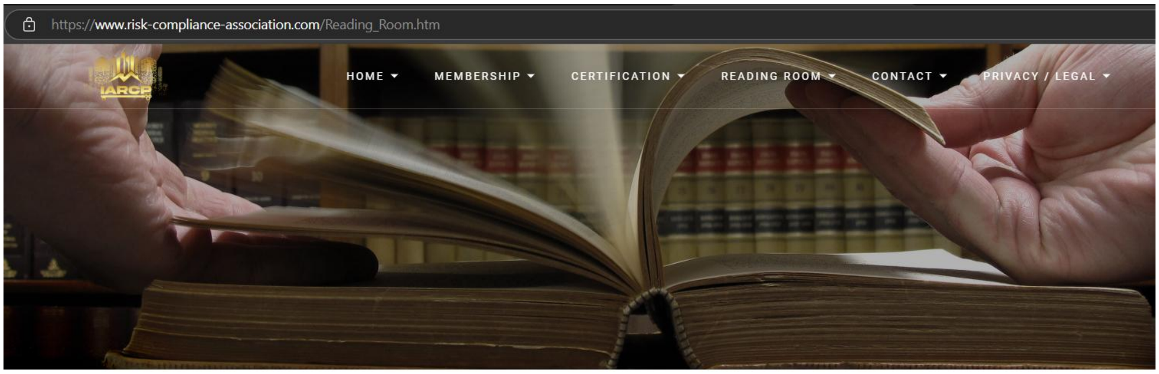
Overview

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

Compliance LLC
TAILOR - MADE TRAINING

IARCP