Monday, April 22, 2023

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.

Financial stress tests are very difficult risk and compliance management exercises.

The European Insurance and Occupational Pensions Authority (EIOPA) has just launched its 2024 stress test. Insurers in the European Economic Area must consider a hypothetical scenario of severe but plausible adverse developments in financial and economic conditions.

For many years we discuss the word plausible. Francis Bacon believed that *truth is so hard to tell, it sometimes needs fiction to make it plausible*. No, Francis was not speaking about financial stress testing.

According to EIOPA, the adverse scenario is based on "the uncertainty deriving from the economic consequences of a re-intensification or prolongation of geopolitical tensions. Such an environment would fuel supply chain disruptions and lead to lower growth and higher inflation.

Second-round effects stemming from a wage-price spiral would further exacerbate inflationary pressures, ultimately leading to a re-appraisal of market expectations of interest rates across tenors and currencies."

We also read: “Households would also experience losses in real income and face higher borrowing costs amid higher unemployment. This would make it challenging for homeowners to service their mortgages, resulting in an increase in mortgage defaults.

The ensuing fall in residential real estate prices is exacerbated by a slowdown in residential property market activity. At the same time, the large increase in interest rates would fuel a disorderly repricing in the commercial real estate market, in the context of structural changes to demand for office space that had been initiated by the COVID-19 pandemic.

The higher cost of debt-servicing, coupled with the sharp fall in property prices, would trigger a sudden repricing of covered bonds and other asset-backed securities, driving spreads upwards.

Such market reactions would also trigger a sudden revaluation of other financial assets in an uncertain environment characterised by high volatility. In particular, equity valuations would drop substantially worldwide, while hedge funds, real estate investment trusts and private equity funds would incur in losses. The latter would be largely affected by an amplification of liquidity stress.

Finally, commodity prices would surge in line with the supply-chain driven inflation prospect.”

Is Europe preparing for war? Friedrich Nietzsche believed that the best weapon against an enemy is another enemy, but EIOPA, the European Insurance and Occupational Pensions Authority, follows the regulatory path. Insurance firms will benefit from this stress test, especially when they make proper assumptions.

Albert Einstein has said: You cannot simultaneously prevent and prepare for war. Well, perhaps Albert was wrong this time. I believe that the opposite is true today.

Read more at number 2 below. Welcome to the Top 10 list.

Best regards,

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

COURT OF JUSTICE
OF THE EUROPEAN UNION

Number 7 (Page 21)

Gas Pipeline Safety: Better Data and Planning Would Improve Implementation of Regulatory Changes

GAO
U.S. Government Accountability Office

Number 8 (Page 23)

Consultation Paper

Draft technical standards and guidelines specifying certain requirements of the Markets in Crypto Assets Regulation (MiCA) on detection and prevention of market abuse, investor protection and operational resilience

ESMA
European Securities and Markets Authority

Number 9 (Page 25)

Fighting cookie theft using device bound sessions

Chromium Blog

Number 10 (Page 29)

Protect Yourself: Commercial Surveillance Tools

Number 1

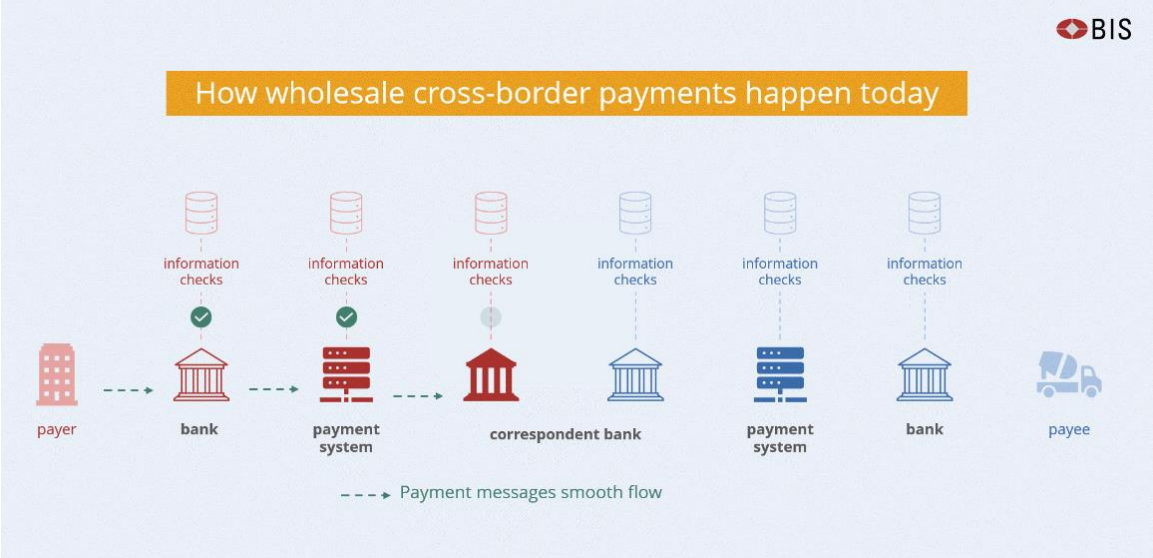
Project Agorá (Greek for "marketplace"): central banks and banking sector embark on major project to explore tokenisation of cross-border payments

The Bank for International Settlements (BIS) together with seven central banks today announced plans to join forces with the private sector to explore how tokenisation can enhance the functioning of the monetary system.

Project Agorá (Greek for "marketplace") brings together seven central banks: Bank of France (representing the Eurosystem), Bank of Japan, Bank of Korea, Bank of Mexico, Swiss National Bank, Bank of England and the Federal Reserve Bank of New York. They will seek to work in partnership with a large group of private financial firms convened by the Institute of International Finance (IIF).

The project builds on the unified ledger concept proposed by the BIS and will investigate how tokenised commercial bank deposits can be seamlessly integrated with tokenised wholesale central bank money in a public-private programmable core financial platform.

This could enhance the functioning of the monetary system and provide new solutions using smart contracts and programmability, while maintaining its two-tier structure.



Smart contracts can enable new ways of settlement and unlock types of transactions that are not viable or practical today, in turn offering new opportunities to benefit businesses and people.

This major public-private partnership will seek to overcome several structural inefficiencies in how payments happen today, especially across borders, which add a layer of challenges: different legal, regulatory and technical requirements,

operating hours and time zones. Plus the increased complexity of carrying out financial integrity controls (eg against money laundering and customer verification), which today are often repeated several times for the same transaction, depending on the number of intermediaries involved.

BIS Innovation Hub projects are generally experimental in nature and aim to explore and deliver public goods to the global central banking community.

Next steps

The BIS will issue a call for expressions of interest to private financial institutions to join Project Agorá. The IIF will act as the intermediary and convener of private sector participants.

It is envisaged that several regulated financial institutions will participate representing each of the seven currencies. Specific instructions and requirements will be issued in due course. Being a member of the IIF is not a requirement to participate.

To read more: https://www.bis.org/about/bisih/topics/fmis/agora.htm

Number 2

EIOPA stress tests European insurers' resilience with a scenario of escalating geopolitical tensions

The European Insurance and Occupational Pensions Authority (EIOPA) is launching its 2024 stress test in which it subjects insurers in the European Economic Area to a hypothetical scenario of severe but plausible adverse developments in financial and economic conditions.

This year's exercise envisions a re-intensification or prolongation of geopolitical tensions and assesses how European insurers would cope with the wide-ranging economic and financial market consequences of such an event.

Objective

While EIOPA's 2024 stress test is not a pass or fail exercise, it has a mostly microprudential orientation.

The goal is primarily to assess the resilience of the participants to the adverse scenario whose shocks go beyond the regular resilience required under Solvency II and provide supervisors with information on whether these insurers are able to withstand severe shocks. EIOPA will also analyze aggregate results to assess potential sector-wide vulnerabilities.

This microprudential approach will enable European and national supervisors to issue recommendations to the industry as a whole, and, where relevant, to discuss potential follow-up actions with individual insurers, to improve their resilience.

The microprudential assessment is complemented by the estimation of potential spillover from the insurance sector to other parts of the financial system, triggered by reactions to the prescribed shocks.

Scenario

The 2024 scenario, developed by EIOPA in close cooperation with the European Systemic Risk Board, presumes a renewed build-up or continuation of geopolitical tensions together with a broad range of knock-on effects.

As a result of high tensions, the narrative envisages a resurgence of widespread supply-chain disruptions, leading to sluggish growth and reigniting inflationary pressures.

The ripple effects include a re-evaluation of interest rate expectations marked by a surge in short-term market rates and more muted increases in longer term yields, further steepening an already inverted yield curve.

The resulting tightening of financing conditions, coupled with subdued growth, is poised to dampen corporate profitability, widen credit spreads, and adversely affect asset classes across the board.

The high level of government bond yields, also driven by sustained high risk-free rates, would tighten financing conditions for public spending.

The pandemic-induced elevated level of government debt and the need for mitigating measures to support the real economy in a downturn would fuel concerns about sovereign debt sustainability, leading to a further heterogenous increase in government bond rates.

Approach and scope

EIOPA has translated the above narrative into a set of market and insurance-specific shocks to assess the insurance industry's resilience to them from a capital as well as from a liquidity perspective.

The sample for the stress test will include 48 undertakings from 20 member states and cover over 75% of the EEA market in terms of total assets.

Timeline

Following the launch, participating undertakings will have until mid-August 2024 to calculate their results based on the prescribed scenario and submit them to the relevant national supervisor.

Once the results are submitted, EIOPA will undertake a quality assurance process to validate the results, which is expected to last until end of October 2024.

Communication of the results

The outcome of the 2024 Stress Test will be published in December in two forms:

- Report based on aggregated data;
- Publication of individual results relating to a subset of capital-based indicators (subject to the consent of the relevant entity).

For more information, go to the dedicated page of the exercise:
https://www.eiopa.europa.eu/insurance-stress-test-2024_en

To read more:
https://www.eiopa.europa.eu/eiopa-stress-tests-european-insurers-resilience-scenario-escalating-geopolitical-tensions-2024-04-02_en

Number 3

Bank Liquidity, Regulation, and the Fed's Role as Lender of Last Resort

Governor Michelle W. Bowman, at The Roundtable on the Lender of Last Resort: The 2023 Banking Crisis and COVID, sponsored by the Committee on Capital Markets Regulation, Washington, D.C.

Today's roundtable comes at an opportune time, as we recently passed the one-year anniversary of the failures of Silicon Valley Bank (SVB) and Signature Bank. The long shadow of these bank failures, and the subsequent failure of First Republic, have prompted a great deal of discussion about the bank regulatory framework, including capital regulation, the approach to supervision, and the role of tailoring, among other topics.

It is my hope that our discussion today reviews and considers the appropriate role of the Federal Reserve in providing liquidity to the U.S. banking system and, of course, its role as the "lender of last resort" through the discount window and authority under section 13(3) of the Federal Reserve Act.

I look forward to today's panels and a deeper examination of important policy questions, including the lessons that should be learned from the banking system stress experienced last spring, the broader stress in financial markets during the COVID-19 crisis, potential approaches to operationally enhance and optimize tools like the discount window to more effectively meet industry liquidity needs, and the importance of effective resolution mechanisms in the banking system.

Before the panels get into a "deep dive" on these policy issues, I would like to briefly touch on three main themes:

(1) the broader framework in which the Federal Reserve supports liquidity in the banking system, particularly how this function complements other regulatory requirements and sources of liquidity;

(2) how this function can be optimized to work within the evolving liquidity framework; and

(3) the challenges we face in making the Federal Reserve's liquidity tools, particularly the discount window, effective.

The Federal Reserve's Role in Banking System Liquidity

The complexity of the U.S. financial system makes it difficult to predict where the next stress (or in the worst case, the next crisis) will arise. While today's event will focus on recent episodes that required the Federal Reserve to employ its liquidity

tools—the COVID crisis and the early 2023 banking stress—it is helpful to consider how the Federal Reserve's authority has evolved in the aftermath of the 2008 financial crisis.

Let's review the historical context, which could be helpful for framing the discussion. In 1913, Congress established the Federal Reserve at least in part to help address the pattern of cyclical financial panics and the ensuing economic turmoil that followed by allowing the Fed to create a more elastic money supply to meet demand for liquidity during times of stress. This authority included tools like open market operations, later used as a tool for monetary policy.

Since its establishment, the Federal Reserve was granted the authority to engage in discount window lending. In addition, during the Great Depression, the Fed was given a broader set of tools to engage in emergency lending under section 13(3) of the Federal Reserve Act.

More recently, in 2003, the Federal Reserve restructured its previous discount window lending programs and established the Primary Credit Facility (PCF) and Secondary Credit Facility.

Primary credit enabled financially strong banks to obtain secured loans from the discount window at a penalty rate. The secondary credit provided discount window loans at a higher rate, and with higher collateral haircuts and other more stringent terms than apply for primary credit, to solvent institutions that did not qualify to borrow from the PCF.

This evolution of the discount window function more closely aligned operations with a theory, often attributed to Walter Bagehot, that central banks should lend freely to solvent institutions against good collateral, at a penalty rate of interest.

The Fed used its lending tools extensively during the 2008 financial crisis. Relying heavily on discount window lending authority and emergency lending facilities under section 13(3) of the Federal Reserve Act, the Fed provided emergency liquidity to support individual firms that were under severe stress, and to facilitate the flow of credit more broadly.

Of course, the financial crisis left a lasting imprint on many Americans who suffered significant economic harm, many of whom have not yet fully recovered. It also prompted Congress to review and amend the Fed's authorities through the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act).

The banking system today is stronger and more resilient than it was before the 2008 financial crisis with significantly more capital and substantially more liquidity. U.S. banks are also subject to a host of supervisory tools that did not exist prior to the Dodd-Frank Act, like new stress testing requirements.

Many of the regulatory changes implemented at that time were designed to reduce the probability of large bank failures, but the statute also mandated other changes designed to improve the likelihood that failing large banks could be resolved without broad systemic disruptions.

Of course, these changes were additive to existing authorities that are meant to promote banking system resilience, particularly the other core element of the federal safety net, deposit insurance.

Congress also made significant changes to the Fed's emergency lending authority. For example, section 13(3) facilities must now be broad-based, rather than designed only for individual firms, and must be approved by the U.S. Treasury Secretary. In addition, loans can only be made to solvent institutions, and there are new collateral and disclosure requirements.

Further, while the Dodd-Frank Act preserved the Fed's ability to make discount window loans to eligible borrowers, including depository institutions and U.S. branches of foreign banks, it made some modifications.

Notably, one change that I will return to later is the new requirement that discount window lending is no longer confidential. These loans, including the names of borrowing institutions, are now required to be disclosed with a two-year lag.

Changes made by the new law and other subsequent changes have attempted to strike a balance between making firms more resilient to stress and adding additional parameters to the Fed's liquidity tools.

The complementary tools we have—the prudential bank regulatory framework, tools to promote banking system liquidity and stability, discount window lending and "lender of last resort" authority, and resolution tools—all contribute to the safety and soundness of individual banks, and more broadly, to financial stability.

Broadly defined, the challenge we face is that banking crises and banking stress can arise from unpredictable events.

They can be the product of external events (like a global pandemic) or can arise from cascading failures of bank management and regulators to identify and effectively address and mitigate the buildup of risk.

This risk can occur at a single institution, like we saw in the lead-up to the failure of SVB, or more broadly throughout the financial system, as we saw during the last financial crisis.

When we consider banking system stress and potential crises in the broader context, our primary goal should always be prevention, particularly so that we can avoid contagion risks that lead to financial instability and more significant government intervention.

We should be reluctant to intervene in private markets, including using emergency government lending facilities to support private enterprises.

The federal safety net that covers the banking system—including discount window lending and deposit insurance—is meant to make the U.S. banking system and broader economy more resilient.

Where market disruptions affect liquidity, it is important that these tools—particularly discount window lending—function effectively.

So, we must ask whether there are steps we can take to optimize the functioning of these tools and identify some of the key challenges we face in making these tools effective, including preserving industry standard access to liquidity outside of the Fed's tools for day-to-day liquidity management, like advances from the Federal Home Loan Banks.

To read more:
https://www.federalreserve.gov/newsevents/speech/bowman20240403a.htm

Number 4

Cybersecurity and Infrastructure Security Agency (CISA), DHS
Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements

AGENCY:
Cybersecurity and Infrastructure Security Agency, DHS

ACTION:
Proposed rule.

SUMMARY:
The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), as amended, requires the Cybersecurity and Infrastructure Security Agency (CISA) to promulgate regulations implementing the statute's covered cyber incident and ransom payment reporting requirements for covered entities.

CISA seeks comment on the proposed rule to implement CIRCIA's requirements and on several practical and policy issues related to the implementation of these new reporting requirements.

DATES:
Comments and related material must be submitted on or before June 3, 2024.

Executive Summary

A. Purpose and Summary of the Regulatory Action

On March 15, 2022, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) was signed into law.

CIRCIA requires covered entities to report to CISA within certain prescribed timeframes any covered cyber incidents, ransom payments made in response to a ransomware attack, and any substantial new or different information discovered related to a previously submitted report.

CIRCIA further requires the Director of CISA to implement these new reporting requirements through rulemaking, by issuing an NPRM no later than March 15, 2024, and a final rule within 18 months of publication of the NPRM. CISA is issuing this NPRM to solicit public comment on proposed regulations that would codify these reporting requirements.

This NPRM is divided into six sections.

Section I—Public Participation describes the process for members of the public to submit comments on the proposed regulations and lists specific topics on which CISA is particularly interested in receiving public comment.

Section II—Executive Summary contains a summary of the proposed regulatory action and the anticipated costs and benefits of the proposed regulations.

Section III—Background and Purpose contains a summary of the legal authority for this proposed regulatory action; an overview of the current regulatory cyber incident reporting landscape; a description of the purpose of the proposed regulations; a discussion of efforts CISA has taken to harmonize these proposed regulations with other Federal cyber incident reporting regulations; a discussion of information sharing activities related to the proposed regulations; and a summary of the comments CISA received in response to an RFI issued by CISA on approaches to the proposed regulations and during listening sessions hosted by CISA on the same topic.

Section IV—Discussion of Proposed Rule includes a detailed discussion of the proposed rule, the justification for CISA's specific proposals, and the alternatives considered by CISA.

Section V—Statutory and Regulatory Analyses contains the analyses that CISA is required by statute or Executive Order to perform as part of the rulemaking process prior to issuance of the final rule, such as the Initial Regulatory Flexibility Analysis and Unfunded Mandates Reform Act analysis.

Section VI contains the proposed regulatory text.

The proposed rule is comprised of 20 sections, §§ 226.1 through 226.20, beginning with a section containing definitions for a number of key terms used throughout the proposed regulation. Among other definitions, § 226.1 includes proposed definitions for the terms used to describe and ultimately scope what types of incidents must be reported to CISA (cyber incident, covered cyber incident, ransom payment, and substantial cyber incident) and the term used to describe the different types of reports that must be submitted (CIRCIA Reports).

The next section of the proposed rule, § 226.2, describes the applicability of the proposed rule to certain entities in a critical infrastructure sector, those entities that are considered covered entities and to whom the operative provisions of the rule would apply.

The next section of the proposed rule, § 226.3, describes the circumstances under which a covered entity must submit a CIRCIA Report to CISA. This includes when a covered entity experiences a covered cyber incident, makes a ransom payment, has another entity make a ransom payment on its behalf, or acquires substantial new or different information after submitting a previous CIRCIA Report.

CISA is proposing three exceptions to these reporting requirements for covered entities, which are in § 226.4 of the proposed regulation and described in Section IV.D in this document.

These exceptions include when a covered entity reports substantially similar information in a substantially similar timeframe to another Federal agency pursuant to an existing law, regulation, or contract when a CIRCIA Agreement is in place between CISA and the other Federal agency; when an incident impacts certain covered entities related to the Domain Name System (DNS); and when Federal agencies are required by the Federal Information Security Modernization Act of 2014 (FISMA) to report incidents to CISA. See § 226.4 of the proposed regulation and Section IV.D of this document.

Section 226.5 of the proposed regulation contains the submission deadlines for the four different types of CIRCIA Reports (Covered Cyber Incident Reports; Ransom Payment Reports; Joint Covered Cyber Incident and Ransom Payment Reports; Supplemental Reports).

These deadlines, including how to calculate them, are discussed further in Section IV.E.iv in this document. Section 226.6 of the proposed regulation sets forth the proposed manner and form of reporting, which CISA proposes to be through a web-based CIRCIA Incident Reporting Form available on CISA's website or in any other manner and form of reporting approved by the Director.

To read more:
https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements

Number 5

SEC Encourages Investors to Plan for Their Financial Future During Financial Capability Month

U.S. SECURITIES AND EXCHANGE COMMISSION

The Securities and Exchange Commission's Office of Investor Education and Advocacy (OIEA) announced that its theme for April's National Financial Capability Month is, "What does your financial future look like? Having a plan can help answer the question."

During the month of April, SEC leadership and staff will highlight the importance of creating a saving and investing plan to help investors meet their financial goals, and will encourage them to take advantage of the free tools and resources available on Investor.gov. Investor education events will take place across the U.S. with various audiences, including students, underrepresented communities, older investors, and the military.

"Investors turn to our capital markets every day, whether to grow a nest egg, plan for retirement, save for an education, or prepare for the inevitable bumps along the way," said SEC Chair Gary Gensler. "To be an informed investor is to be a more effective investor, and I encourage the public to take advantage of the many resources we offer on Investor.gov."

Some of the SEC's latest resources to educate investors about the importance of financial capability and avoiding fraud, include:

- April's Financial Capability Month Investing Quiz;
- A new Guide for Older Investors;
- A Military Investor Bulletin, "Making the Most of Lump Sum Benefits";
- An Investor Alert: "Artificial Intelligence (AI) and Investment Fraud"; and
- An article from OIEA Director Lori Schock, "Loud (and Proud) Budgeting May Help You Stick To Your Saving and Investing Plan"

"The loud budgeting concept can be an empowering way to take control of your financial future," said Director Lori Schock. "Creating a saving and investing plan that helps you meet your financial goals and sharing those ideals and goals with your family and friends may not only help you stay more committed to your decision-making but can provide you with support to help you stick with your plan for the long term."

Some of the SEC's events planned for Financial Capability Month, include reaching out to the following:

Older Investors – As part of its ongoing Never Stop Learning initiative, OIEA leadership and staff will participate in interviews, webinars, and other events aimed at providing investor education and fraud prevention resources to older investors.

OIEA leadership will appear on a Facebook Live event with the AARP Fraud Watch Network and The Senior Zone radio program. SEC regional office and headquarters staff will conduct webinars and give presentations to older adults at public libraries and community centers.

High School and College Students – OIEA staff will lead financial education activities for high school and college students throughout the month. OIEA staff will present to Washington, D.C., public high school students, leading lessons on investor education basics and concepts like the power of compound growth and avoiding scams.

Staff will engage with additional schools to educate high school students about the importance of building wealth throughout their lifetime and help them realize the benefits of starting young to grow their money over time. OIEA staff will give guest lectures to college students at Haskell Indian Nations University, Kansas State University, and Dalton State College.

Guest lectures will cover investor education topics, such as the relationship between paying down debt, saving and investing, how to avoid fraud, and the importance of creating a saving and investing plan. OIEA staff will also join financial education events for students and young adults hosted by the New York City Bar Association. SEC regional office and headquarters staff will also present

to Historically Black College and University student groups at Morgan State University and other universities and community colleges.

Service Members – OIEA staff will present to service members at military installations across the country. Programs will focus on building wealth, protecting investments by recognizing and avoiding scams, and discussing the benefits of tax-advantaged retirement plans, including the military's Thrift Savings Plan.

Outreach events will include active duty, reserve, and retired service members, as well as veterans and military families. This work builds on the SEC's ongoing investor education outreach with service members, veterans, and their families.

Community Organizations and Affinity Groups – OIEA staff will conduct "train the trainer" sessions for financial educators at the Creating Assets, Savings and Hope (CASH) Campaign of Maryland Financial Education Summit.

OIEA staff will also present a Building Wealth Over Time workshop to Howard County, Maryland, community members as part of their Money Matters community event series. OIEA staff will participate in a Washington, D.C., job training and life skills event for formerly incarcerated citizens. SEC regional office and headquarters staff will engage in dozens of outreach events across the country, including investor education presentations to employee groups, women's groups, and more.

To read more: https://www.sec.gov/news/press-release/2024-43

Number 6

Amazon's request to suspend its obligation to make an advertisement repository publicly available is rejected

COURT OF JUSTICE
OF THE EUROPEAN UNION

Order of the Vice-President of the Court in Case C-639/23 P(R) | Commission v Amazon Services Europe

Amazon Services Europe belongs to the Amazon group. Its business activities comprise online retail and other services such as cloud computing and digital streaming. It provides marketplace services to third-party sellers enabling them to offer products for sale via Amazon Store.

By a decision of 23 April 2023, adopted under the Regulation on a Single Market for Digital Services, the Commission designated Amazon Store as a very large online platform. That means, in particular, that Amazon Store is obliged to make publicly available a repository containing detailed information 3 on its online advertising.

Amazon sought the annulment of that decision before the General Court of the European Union. It had also made an application for interim measures. By order of 27 September 2023, the President of the General Court ordered suspension of the operation of that decision in so far as Amazon Store will be required to make the advertisement repository publicly available. The Commission lodged an appeal before the Court of Justice against that order.

In his order today, *the Vice-President of the Court of Justice sets aside the part of the order of the President of the General Court suspending the Commission's decision in so far as it concerns the advertisement repository*.

He finds that the Commission was denied, in breach of the principle that the parties should be heard, the opportunity to comment on the arguments put forward by Amazon during the proceedings before the General Court. Since the Commission presented to the Court of Justice the arguments that it intended to make against the elements put forward by Amazon before the General Court, *the Vice-President of the Court of Justice gives final judgment in the dispute and dismisses the application for interim measures*.

The Vice-President of the Court considers that Amazon's argument that the obligation introduced by the EU legislature to make an advertisement repository publicly available unlawfully limits its fundamental rights to respect for private life and the freedom to conduct a business, cannot be regarded, prima facie, as irrelevant and, moreover, as lacking in seriousness.

Furthermore, in the absence of a suspension, it is likely that Amazon would suffer serious and irreparable harm before the intervention of any judgment annulling the Commission's decision.

Those findings are not however decisive in themselves. It is necessary to assess whether the balancing of all the interests involved may justify refusing suspension. In that regard, the Vice-President of the Court finds that, in the event that suspension is not granted, the annulment of the Commission's decision would retain an interest for Amazon.

In addition, it has not been demonstrated that, in such a situation, Amazon's existence or long-term development would be jeopardised. Moreover, suspension would lead to a delay, potentially for several years, in the full achievement of the objectives of the Regulation on a Single Market for Digital Services and therefore potentially allow an online environment threatening fundamental rights to persist or develop, whereas the EU legislature considered that very large platforms play an important role in that environment.

The interests defended by the EU legislature prevail, in the present case, over Amazon's material interests, with the result that the balancing of interests weighs in favour of rejecting the request for suspension.

NOTE: The General Court will deliver final judgment on the substance of this case at a later date. An order as to interim measures is without prejudice to the outcome of the main proceedings.

Unofficial document for media use, not binding on the Court of Justice.

To read more:
https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-03/cp240060en.pdf

Full text: https://curia.europa.eu/juris/documents.jsf?num=C-639/23%20P(R)

Number 7

Gas Pipeline Safety: Better Data and Planning Would Improve Implementation of Regulatory Changes

GAO
U.S. Government Accountability Office

About 300,000 miles of natural gas transmission pipelines across the United States carry products from processing facilities to communities and other large volume customers.

Pipelines are a relatively safe mode for transporting natural gas, but incidents can still occur that result in death, injury, and property and environmental damage. The Department of Transportation's Pipeline and Hazardous Materials Safety Administration (PHMSA) sets the federal minimum safety standards for these pipelines.

In 2003, PHMSA established integrity management—a risk-based approach to managing certain gas transmission pipelines—as an addition to its existing pipeline safety regulations.

Under this approach, operators are required to assess pipelines in high consequence areas (HCA)—generally, areas where an incident could have the greatest impact to public safety or property—to identify threats and mitigate risks.

In October 2019 and August 2022, PHMSA issued final rules that both strengthened its gas transmission pipeline safety regulations and expanded some integrity assessment requirements beyond HCAs, including to newly defined moderate consequence areas (MCA).

The Protecting our Infrastructure of Pipelines and Enhancing Safety Act of 2016 includes a provision for us to examine gas transmission integrity management programs following PHMSA's completion of a specific pipeline safety rulemaking.

We are providing information on potential changes to the methods operators use to identify HCAs; how selected stakeholders, including pipeline operators and state inspectors, view the regulatory changes to gas transmission pipeline safety; and how PHMSA is overseeing the implementation of the 2019 and 2022 final rules stemming from the rulemaking.

What are gas transmission pipelines?

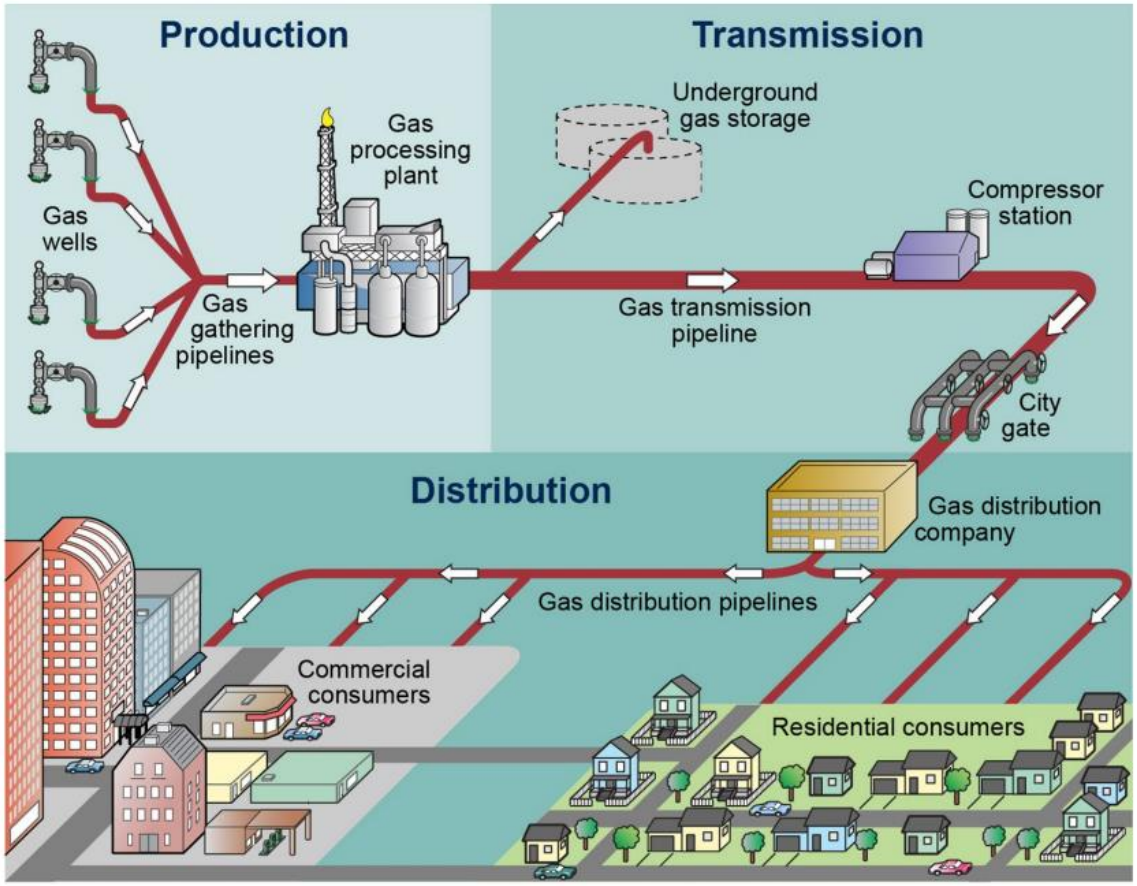
Natural gas transmission pipelines carry gas, sometimes over hundreds of miles, to communities and large-volume users (e.g., factories).

In 2023, PHMSA officials estimated that the United States has over 300,000 miles of onshore gas transmission pipelines. Roughly two-thirds of these miles were interstate pipelines, or pipelines that generally cross state boundaries.

The remaining third were intrastate pipelines, or pipelines that tend to operate within a single state.

Transmission pipelines tend to have larger diameters and operate at higher pressures than other types of pipelines (see fig.1).

Figure 1: Transmission Pipelines within a Natural Gas Pipeline System



Source: GAO analysis of Energy Information Administration and Natural Gas Council documents; GAO (illustration). | GAO-24-106690

To read more: https://www.gao.gov/products/gao-24-106690

Number 8

Consultation Paper

Draft technical standards and guidelines specifying certain requirements of the Markets in Crypto Assets Regulation (MiCA) on detection and prevention of market abuse, investor protection and operational resilience

Reasons for publication

The Regulation on markets in crypto-assets (MiCA) was published in the Official Journal of the EU on 9 June 2023.

The European Securities and Markets Authority (ESMA) has been empowered to develop technical standards and guidelines specifying certain provisions.

ESMA published a first consultation package in July 2023, a second in December 2023 and two additional standalone consultation papers in January 2024.

This latest consultation package (no. 3) includes all remaining mandates with an 18-month deadline.

The aim of these public consultations is to collect views, comments, and opinions from stakeholders, investors and market participants on the appropriate implementation of MiCA.

Article 92(2) of MiCA:

"ESMA shall develop draft regulatory technical standards to further specify:

(a) appropriate arrangements, systems and procedures for persons to comply with paragraph 1;

(b) the template to be used by persons to comply with paragraph 1;

(c) for cross-border market abuse situations, coordination procedures between the relevant competent authorities for the detection and sanctioning of market abuse"

Contents

This paper contains 4 sections (chapters 3 – 6) relating to the four mandates under consultation:

(i) prevention and detection of crypto-asset market abuse;

(ii) suitability requirements applicable to the provision of advice and portfolio management services in crypto-assets and the format of the periodic statement to be provided for portfolio management services;

(iii) transfer services for crypto-assets; and

(iv) maintenance of systems and security access protocols.

An aggregated list of consultation questions can be found in Annex I. Annex II includes the draft RTS and guidelines.

Next Steps

ESMA aims to close the public consultation respecting legal deadlines as set out in MiCA. ESMA will consider the feedback received during this consultation and expect to publish a final report and submit the draft technical standards to the European Commission for endorsement by December 2024.

Article 2

General requirements

1. Persons professionally arranging or executing transactions in crypto-assets shall establish and maintain arrangements, systems and procedures that ensure:

   (a) effective and ongoing monitoring of all orders received and transmitted, and all transactions in crypto-assets executed, for the purposes of preventing, detecting and identifying orders and transactions that could constitute market abuse;

   (b) effective and ongoing monitoring, for the purposes of detecting and identifying other aspects of the functioning of the distributed ledger technology, such as the consensus mechanism, where there might exist circumstances indicating that market abuse has been committed, is being committed or is likely to be committed;

   (c) the transmission of STORs to competent authorities in accordance with the requirements set out in this Regulation and using the template set out in the Annex.

2. The obligations referred to in paragraph 1 shall apply to orders, transactions and other aspects of the functioning of the distributed ledger technology which might constitute market abuse and shall apply irrespective of:

Note: Suspicious transaction and order report (STOR) means the report on suspicious orders or transactions, including any cancellation or modification thereof, and other aspects of functioning of the distributed ledger technology where there might exist circumstances indicating that market abuse has been committed, is being committed or is likely to be committed;

To read more:
https://www.esma.europa.eu/sites/default/files/2024-03/ESMA75-453128700-1002_MiCA_Consultation_Paper_-_RTS_market_abuse_and_GLs_on_investor_protection_and_operational_resilience.pdf

Number 9

Fighting cookie theft using device bound sessions

Chromium Blog

Note: The Chromium projects include Chromium and ChromiumOS, the open-source projects behind the Google Chrome browser and Google ChromeOS.

Cookies – small files created by sites you visit – are fundamental to the modern web. They make your online experience easier by saving browsing information, so that sites can do things like keep you signed in and remember your site preferences. Due to their powerful utility, cookies are also a lucrative target for attackers.

Many users across the web are victimized by cookie theft malware that gives attackers access to their web accounts.

Operators of Malware-as-a-Service (MaaS) frequently use social engineering to spread cookie theft malware. These operators even convince users to bypass multiple warnings in order to land the malware on their device.

The malware then typically exfiltrates all authentication cookies from browsers on the device to remote servers, enabling the attackers to curate and sell the compromised accounts.

Cookie theft like this happens after login, so it bypasses two-factor authentication and any other login-time reputation checks. It's also difficult to mitigate via anti-virus software since the stolen cookies continue to work even after the malware is detected and removed.

And because of the way cookies and operating systems interact, primarily on desktop operating systems, Chrome and other browsers cannot protect them against malware that has the same level of access as the browser itself.

To address this problem, we're prototyping a new web capability called Device Bound Session Credentials (DBSC) that will help keep users more secure against cookie theft.

The project is being developed in the open at github.com/WICG/dbsc with the goal of becoming an open web standard.

By binding authentication sessions to the device, DBSC aims to disrupt the cookie theft industry since exfiltrating these cookies will no longer have any value.

We think this will substantially reduce the success rate of cookie theft malware.

Attackers would be forced to act locally on the device, which makes on-device detection and cleanup more effective, both for anti-virus software as well as for enterprise managed devices.

Learning from prior work, our goal is to build a technical solution that's practical to deploy to all sites large and small, to foster industry support to ensure broad adoption, and to maintain user privacy.

Technical solution

At a high level, the DBSC API lets a server start a new session with a specific browser on a device.

When the browser starts a new session, it creates a new public/private key pair locally on the device, and uses the operating system to safely store the private key in a way that makes it hard to export.

Chrome will use facilities such as Trusted Platform Modules (TPMs) for key protection, which are becoming more commonplace and are required for Windows 11, and we are looking at supporting software-isolated solutions as well.

The API allows a server to associate a session with this public key, as a replacement or an augmentation to existing cookies, and verify proof-of-possession of the private key throughout the session lifetime.

To make this feasible from a latency standpoint and to aid migrations of existing cookie-based solutions, DBSC uses these keys to maintain the freshness of short-lived cookies through a dedicated DBSC-defined endpoint on the website.

This happens out-of-band from regular web traffic, reducing the changes needed to legacy websites and apps.

This ensures the session is still on the same device, enforcing it at regular intervals set by the server. For current implementation details please see the public explainer.

Preserving user privacy

Each session is backed by a unique key and DBSC does not enable sites to correlate keys from different sessions on the same device, to ensure there's no persistent user tracking added.

The user can delete the created keys at any time by deleting site data in Chrome settings. The out-of-band refresh of short-term cookies is only performed if a user is actively using the session (e.g. browsing the website).

DBSC doesn't leak any meaningful information about the device beyond the fact that the browser thinks it can offer some type of secure storage.

The only information sent to the server is the per-session public key which the server uses to certify proof of key possession later.

We expect Chrome will initially support DBSC for roughly half of desktop users, based on the current hardware capabilities of users' machines.

We are committed to developing this standard in a way that ensures it will not be abused to segment users based on client hardware.

For example, we may consider supporting software keys for all users regardless of hardware capabilities. This would ensure that DBSC will not let servers differentiate between users based on hardware features or device state (i.e. if a device is Play Protect certified or not).

DBSC will be fully aligned with the phase-out of third-party cookies in Chrome. In third-party contexts, DBSC will have the same availability and/or segmentation that third-party cookies will, as set by user preferences and other factors.

This is to make sure that DBSC does not become a new tracking vector once third-party cookies are phased out, while also ensuring that such cookies can be fully protected in the meantime.

If the user completely opts out of cookies, third-party cookies, or cookies for a specific site, this will disable DBSC in those scenarios as well.

Improving user protection

We are currently experimenting with a DBSC prototype to protect some Google Account users running Chrome Beta. This is an early initiative to gauge the reliability, feasibility, and the latency of the protocol on a complex site, while also providing meaningful protection to our users.

When it's deployed fully, consumers and enterprise users will get upgraded security for their Google accounts under the hood automatically. We are also working to enable this technology for our Google Workspace and Google Cloud customers to provide another layer of account security.

This prototype is integrated with the way Chrome and Google Accounts work together, but is validating and informing all aspects of the public API we want to build.

Interest outside Google

Many server providers, identity providers (IdPs) such as Okta, and browsers such as Microsoft Edge have expressed interest in DBSC as they want to secure their users against cookie theft.

We are engaging with all interested parties to make sure we can present a standard that works for different kinds of websites in a privacy preserving way.

Where to follow the progress

Development happens on GitHub and we have published an estimated timeline. This is where we will post announcements and updates to the expected timelines as needed.

Our goal is to allow origin trials for all interested websites by the end of 2024. Please reach out if you'd like to get involved.

We welcome feedback from all sources, either by opening a new issue or starting a discussion on GitHub.

To read more:
https://blog.chromium.org/2024/04/fighting-cookie-theft-using-device.html

Number 10

Protect Yourself: Commercial Surveillance Tools

Companies and individuals have been selling commercial surveillance tools to governments and other entities that have used them for malicious purposes.

Journalists, dissidents, and other persons around the world have been targeted and tracked using these tools, which allow malign actors to infect mobile and internet-connected devices with malware over both WiFi and cellular data connections.

In some cases, malign actors can infect a targeted device with no action from the device owner.

In others, they can use an infected link to gain access to a device.

These surveillance tools can:

• Record audio, including phone calls.

• Track phone's location.

• Access and retrieve virtually all content on a phone, including text messages, files, chats, commercial messaging app content, contacts, and browsing history.

Below are common cybersecurity practices that may mitigate some risks:

• Regularly update device operating systems and mobile applications.

• Be suspicious of content from unfamiliar senders, especially those which contain links or attachments.

• Don't click on suspicious links or suspicious emails and attachments.

• Check URLs before clicking links, or go to websites directly.

• Regularly restart mobile devices, which may help damage or remove malware implants.

• Encrypt and password protect your device.

• Maintain physical control of your device when possible.

• Use trusted Virtual Private Networks.

• Disable geo-location options and cover camera on devices.

• While these steps mitigate risks, they don't eliminate them. It's always safest to behave as if the device is compromised, so be mindful of sensitive content.

From 2011 to 2023, at least 74 countries contracted with private companies to obtain commercial spyware, which governments are increasingly using to target dissidents and journalists," per the 2024 IC Annual Threat Assessment.

Digital Authoritarianism and Transnational Repression

Foreign states are advancing digital and physical means to repress individual critics and diaspora communities abroad, including in the United States, to limit their influence over domestic publics. States are also growing more sophisticated in digital influence operations that try to affect foreign publics' views, sway voters' perspectives, shift policies, and create social and political upheaval. Digital technologies have become a core component of many governments' repressive toolkits even as they continue to engage in physical acts of transnational repression, including assassinations, abductions, abuse of arrest warrants and familial intimidation. The PRC probably is the top perpetrator of physical transnational repression.

- During the next several years, governments are likely to exploit new and more intrusive technologies—including generative AI—for transnational repression. From 2011 to 2023, at least 74 countries contracted with private companies to obtain commercial spyware, which governments are increasingly using to target dissidents and journalists.

- PRC expatriates have faced accusations of false bomb threats in countries around the world, resulting in local police investigations, revoked visas, placement on travel blacklists, and sometimes detention, as means to harass dissidents overseas. The PRC also probably will seek to maintain its public security bureaus also known as "overseas police stations" to monitor and repress the Chinese diaspora.

To read more:
https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_Jan-7-2022_Protect_Yourself_Commercial_Surveillance_Tools.pdf

Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

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

- should not be relied on in the 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 an interpretative document;

- 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.

The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

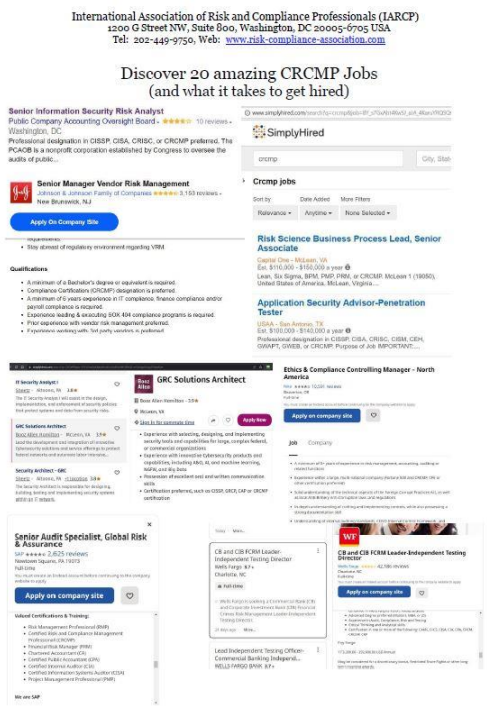
International Association of Risk and Compliance Professionals (IARCP)

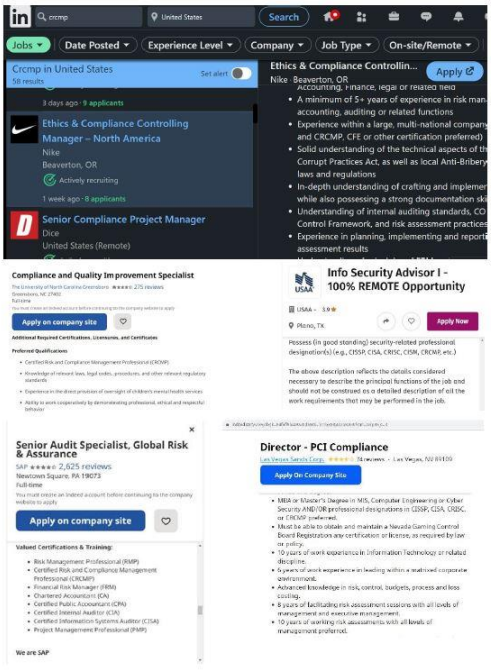
Our training and certification programs:

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 57 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. 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

3. 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

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

5. 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

The International Association of Risk and Compliance Professionals (IARCP) is a business unit of Compliance LLC, incorporated in Wilmington NC and offices in Washington DC, a provider of risk and compliance training and executive coaching in 57 countries. To learn more: https://www.risk-compliance-association.com/Privacy.htm

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
Email: lekatis@risk-compliance-association.com
Web: www.risk-compliance-association.com
HQ: 1220 N. Market Street Suite 804,
Wilmington DE 19801, USA