Monday, April 29, 2024

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.

Aristotle believed that *the secret to humor is surprise.* I have no excuse, but I am still *surprised* when I read: "this guide is aimed at data protection officers (DPO), chief information security officer (CISO) and computer scientists. Privacy lawyers will also be able to find useful elements."

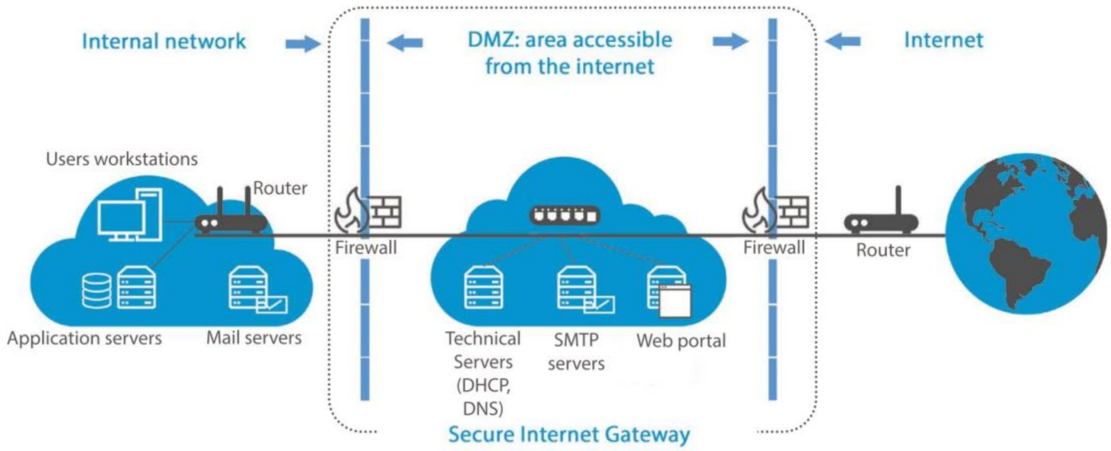
Ten years ago, this would be a joke. There were no papers for privacy lawyers and computer scientists. But this one is not a joke, and I found it very useful. This is a guide from the French data protection authority (CNIL) on the issue of data security, "a living tool that is enriched by state-of-the-art practices and doctrine elements".

According to the guide, "Only allow access to data that the user really needs. Respecting the principle of least privilege, through the management of the authorisation profiles, allows to limit the consequences of an error of manipulation."

Well, the Principle of Least Privilege (PoLP), necessary for highly sensitive environments to ensure that access is strictly limited to individuals who absolutely need access to perform their duties, is now used for privacy and personal information protection. Granting a user more privileges than necessary is a privacy issue too.

Ten years ago, we would not find the words privacy protection and demilitarized zone in the same sentence. We read in the guide:

“Partition the network to mitigate potential security breaches impacts. Implement at least two distinguished network areas: an internal network where no Internet connection is allowed and a DMZ (demilitarized zone) accessible from the Internet, separated by gateways.”



After that I will not be surprised if in the next “Guide 2025” we read that for privacy protection, we also need honeypots (as they are used in network security, not espionage).

Honeypots in network security are decoy systems designed to attract cyber attackers, allowing security professionals to study attack methods, identify attackers, and improve defenses.

Honeypots in espionage are men or women used to entice, seduce, or otherwise manipulate targets to extract information or influence their actions. This involves human interaction and psychological manipulation. Well, the guide was produced in France, but it does not cover fields like that.

As Monica Bellucci (note: not a risk and compliance expert) has said: “In France, they call the beauty of youth “the evil beauty.” You don't have it because of you but because you're born with it. The other kind of beauty is your own work, and it takes forever.”

Well, the French guide is talking *about the other kind of beauty, our own work, and I am afraid it really takes forever* to comply with the new privacy regulations and guides.

Read more at number 1 below. Welcome to the Top 10 list.

Best regards,

George Lekatis
President of the IARCP

Number 7 (Page 21)

Revisiting the Non-Paper

Non-Paper on EU Cyber Diplomacy, by Estonia, France, Germany, Poland, Portugal and Slovenia

Federal Foreign Office

Auswärtiges Amt

Number 8 (Page 26)

CISA Issues Emergency Directive 24-02: Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Number 9 (Page 27)

Listening to the Data: How a NIST Tool Helps Labs Worldwide Harmonize Measurements

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Number 10 (Page 30)

Lawrence Livermore National Laboratory (LLNL) - See the solar corona: an intricate pattern reveals itself during the April 8 eclipse

Number I

CNIL and the application of the EU GDPR to Artificial Intelligence

Note: CNIL is the French National Commission on Information Technology and Liberties. It was created in January 1978.

The objective of this guide is to support organisations in the implementation of security measures in order to ensure the protection of personal data. It is aimed in particular at data protection officers (DPO), chief information security officer (CISO) and computer scientists. Privacy lawyers will also be able to find useful elements.

This guide is a living tool that is enriched by state-of-the-art practices and doctrine elements of the French data protection authority (CNIL) on the issue of data security. A changelog is available on the CNIL website to help actors identify the evolutions that need to be taken into account in order to adapt their level of security.

Security is an essential part of the protection of personal data. It is binding on any data controller and data processor through Article 32 of the General Data Protection Regulation (GDPR).

In principle, each processing operation must be subjected to a set of security measures decided according to the context, namely “useful precautions, having regard to the nature of the data and the risks presented by the processing” (Article 121 of the French Data Protection Act).

The GDPR specifies that the protection of personal data requires taking “appropriate technical and organisational measures to ensure a level of security appropriate to the risk” for the rights and freedoms of natural persons, including their privacy.

To assess the measures to be put in place, two complementary approaches are to be deployed:

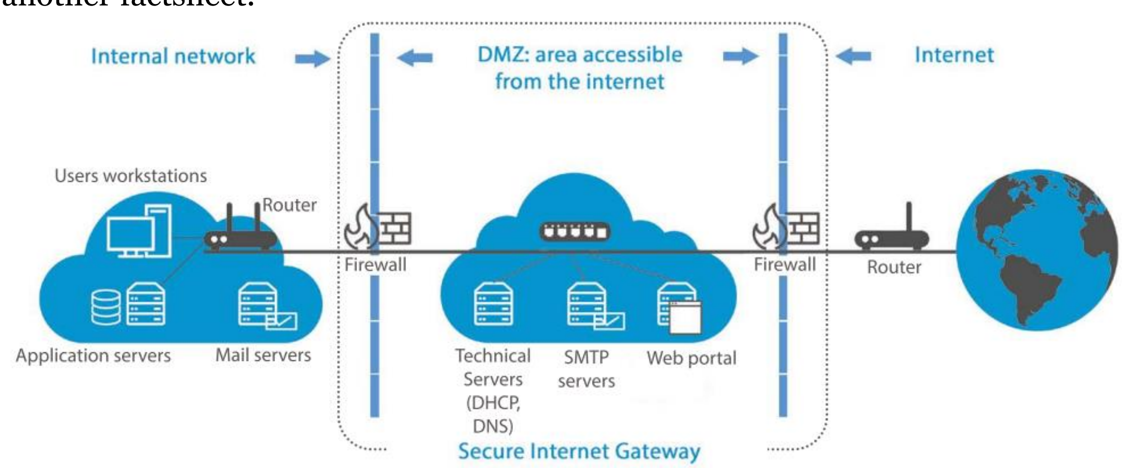
– the establishment of a security base incorporating good practices resulting from years of capitalising on hygiene and IT security (e.g.: regulations, standards, guides). This base aims to address the most common risks;

– the risk analysis for the persons concerned by the processing, which aims to identify and assess the risks specific to the treatment. Such an analysis supports objective decision-making on the treatment of these risks and the identification of necessary and context-appropriate measures. However, it is difficult for non-specialists in IT security to implement such an approach and to ensure that the level of security of the processing for which they are responsible is sufficient.

To help with compliance, this guide presents a set of recommendations grouped by thematic factsheets. Each factsheet is structured in three sections:

– basic precautions, which incorporate essential good practices;
– bad trend practices, which should be avoided;
– additional measures, to go further.

Each factsheet can be read separately from the others: references are given when another factsheet.



Example of a confidentiality commitment clause for individuals who are intended to manipulate personal data

I, the undersigned Mr/Mrs. exercising the functions of____ within the company_______________________(hereinafter referred to as "the Company"), being therefore required to access personal data, declares that I recognise the confidentiality of such data.

I therefore undertake, in accordance with Article 32 of the General Data Protection Regulation of 27 April 2016, to take all precautions in accordance with the state of the art and internal rules within the framework of my powers in order to protect the confidentiality of the information to which I have access, and in particular to prevent it from being communicated to persons not expressly authorised to receive such information.

In particular, I undertake to:

- not to use the data that I can access for purposes other than those provided for by my powers;
- disclose this data only to persons duly authorised, by reason of their functions, to receive such information, whether private, public, natural or legal;
- not to make any copies of this data except as necessary for the performance of my duties;
- take all measures consistent with the state of the art and internal rules within the framework of my powers in order to avoid the misuse or fraudulent use of this data;
- take all precautions in accordance with the state of the art and internal rules to preserve the physical and logical security of this data;
- ensure, within my powers, that only secure means of communication will be used to transfer this data;
- in the event of termination of my duties, return in full the data, computer files and any information media relating to these data.

This confidentiality commitment, in force for the duration of my duties, will remain effective, after the termination of my duties, whatever the cause and until the data has been made public by the Company, provided that this commitment concerns the use and communication of personal data.

I have been informed that any breach of this undertaking exposes me to disciplinary and criminal sanctions in accordance with the regulations in force, in particular with regard to Articles 226-13 and 226-16 to 226-24 of the Criminal Code.

Done at xxx, xxx, in xxx copies

Name:
Signature:

To read more:
https://www.cnil.fr/sites/cnil/files/2024-03/cnil_guide_securite_personnelle_ven_0.pdf

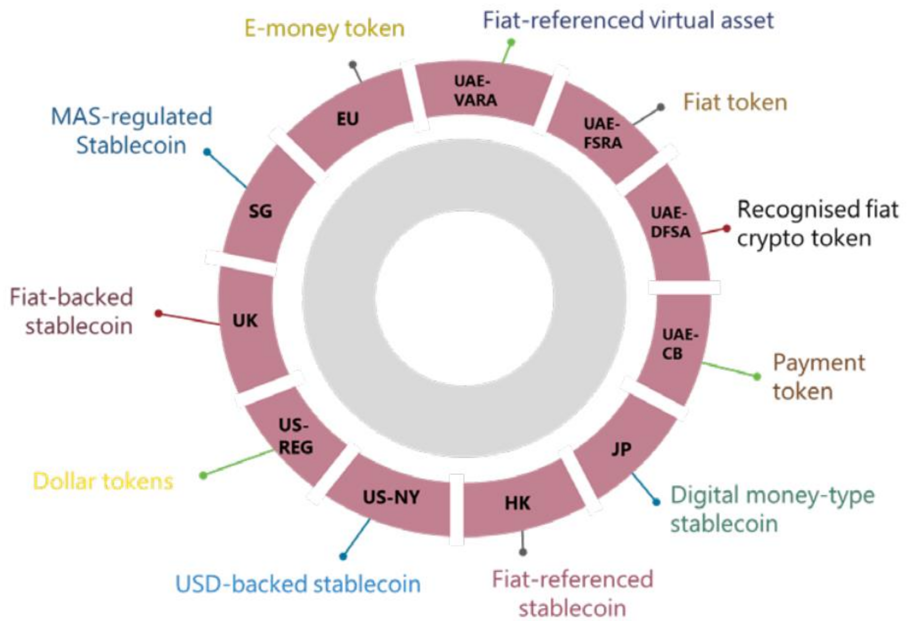
Number 2

Stablecoins: regulatory responses to their promise of stability

Juan Carlos Crisanto, Johannes Ehrentraud and Denise Garcia Ocampo
Financial Stability Institute (FSI) Insights on policy implementation No 57

BIS

Stablecoin terminology used across regulatory frameworks — Graph 2



For further details, see Annex 2.

Source: FSI staff.

In contrast to other cryptoassets, stablecoins come with a promise of stability.

Their issuers promise that they can maintain parity relative to a referenced asset and be redeemed upon request.

Among various types, stablecoins that are pegged to a single currency, such as the US dollar, and backed by traditional financial assets have the potential to be widely used as a means of payment.

Due to this potential, they are increasingly entering mainstream finance, and a number of jurisdictions have developed regulatory approaches for issuers of stablecoins pegged to a single fiat currency.

While stablecoins might bring a range of benefits, they also introduce significant risks.

Proponents argue that they have the potential to increase financial inclusion, reduce costs and enhance the efficiency of cross-border payments. Yet many benefits remain theoretical.

Instances of stablecoins de-pegging and, in some cases, collapsing have occurred, undermining their promised stability. Moreover, their role in illicit activities and potential to threaten financial stability, especially if their ties to traditional finance deepen, raise concerns.

Many regulatory approaches have similar key requirements for stablecoin issuers.

Most follow two types of authorisation regimes that allow stablecoins to be issued by:

(i) banks and certain nonbank financial institutions; and/or

(ii) a new type of financial entity holding a crypto-specific licence.

Issuers are widely required to maintain reserves in segregated accounts equal to the value of their stablecoins in circulation.

Regulations generally emphasise prudential, governance, risk management, anti-money laundering and countering the financing of terrorism (AML/CFT) and disclosure requirements, and providing clear information to stablecoin holders.

However, there are relevant differences in regulatory regimes that could lead to a lack of consistency and coordination in the oversight of stablecoins across jurisdictions.

The terminology used to define in-scope stablecoins varies significantly across regulations. There are also notable differences in the specifics of the regulatory treatment of reserves, and in relation to segregation and custody.

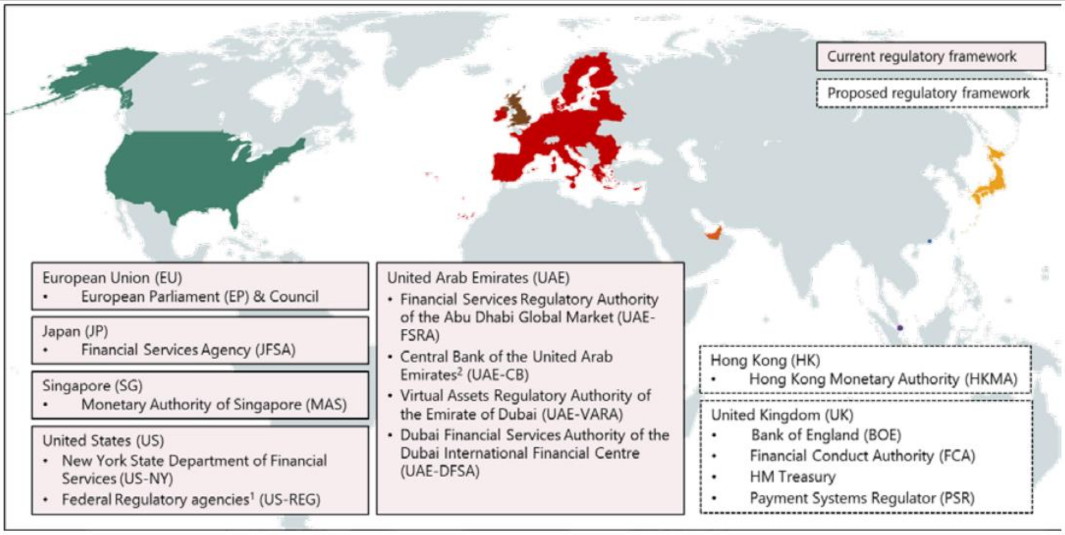
Despite common expectations about redemption policies, the nature of stablecoin holders' claims varies across regimes, as well as the treatment of redemption fees.

As the adoption of stablecoins increases, preventing regulatory fragmentation and achieving a harmonious coexistence of different types of digital assets will become more important.

Authorities face the challenge of establishing a regulatory framework that encourages innovation while mitigating risks. Therefore, as stablecoin markets develop, international cooperation will be critical to shape an effective and consistent regulatory environment for stablecoins.

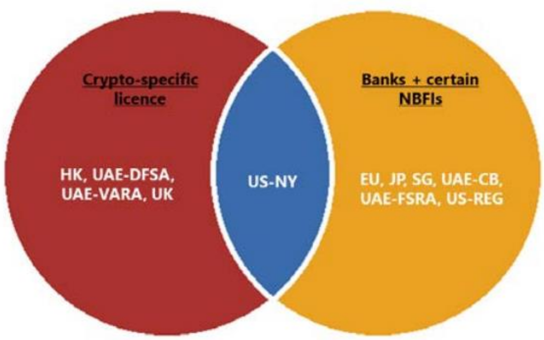
In addition, the interoperability of stablecoins with other digital assets, such as central bank digital currencies (CBDCs) and tokenised deposits, will help to facilitate an integrated global financial system.

Scope: current and proposed regulatory frameworks Graph 1



[1] US regulatory agencies include the Federal Reserve System, the Federal Deposit Insurance Corporation (FDIC) and the Office of the Comptroller of the Currency (OCC). [2] The analysis of the regulatory framework by the UAE-CB is based on the Retail Payment Services and Card Schemes Regulation referred to in Annex 1. The authors acknowledge that a new regulation on payment token services is coming out soon, which may supersede some of the requirements outlined in this paper.

Licensing regimes Graph 3



Jurisdiction	Licence type
EU	Credit institution or electronic money institution/ELMI
HK	Fiat-referenced stablecoin (FRS) licence
JP	Bank, fund transfer service provider or trust company
SG	Bank or "Major Payment Institution licence"
UAE-CB	Bank or "Payment Service Provider licence"
UAE-DFSA	Recognised fiat crypto token
UAE-FSRA	"Financial Services Permission" (FSP) for providing money services
UAE-VARA	Licence Category 1 – "VA issuance"
UK	A new regulated activity will be created under the Regulated Activities Order (RAO) for SC issuance.
US-NY	Licence to engage in virtual currency business activity – "BitLicense" or "Limited Purpose Trust Company Charter"
US-REG	National banks, state member banks, and all insured depository institutions

NBFI = non-bank financial institution. See Annex 3.

Source: FSI staff.

To read more: https://www.bis.org/fsi/publ/insights57.pdf

Number 3

Cyber Resilience Act Requirements Standards Mapping

The increasing number of cyberattacks affecting digital products, coupled with widespread vulnerabilities and insufficient timely security updates, creates heavy financial burdens on society.

In response, the European Commission has drafted the Cyber Resilience Act (CRA), a new proposal for regulation to define the legislative framework of essential cybersecurity requirements that manufacturers must meet when placing any product with digital elements on the internal market.

To facilitate adoption of the CRA provisions, these requirements need to be translated into the form of harmonised standards, with which manufacturers can comply.

In support of the standardisation effort, this study attempt to identify the most relevant existing cybersecurity standards for each CRA requirement, analyses the coverage already offered on the intended scope of the requirement and highlights possible gaps to be addressed.

Introduction

On 15 September 2022, the European Commission published the proposal for the Cyber Resilience Act (CRA), a proposal for a first ever EU-wide legislation of its kind, aimed at introducing mandatory cybersecurity requirements for products with digital elements throughout their lifecycle.

The CRA proposal covers all products with digital elements put on the market which can be connected to a device or a network, including their building blocks (i.e., hardware and software) and encompassing also solutions provided in a Software as a Service (SaaS) fashion if they qualify as remote data processing solutions, as defined by Article 3(2) of the CRA proposal.

The CRA proposal provides two sets of essential requirements:

— Product cybersecurity requirements in Annex I, Section 1 of the CRA proposal

— Vulnerability handling process requirements in Annex I, Section 2 of the CRA proposal

These requirements should be the subject of a standardisation process by the European Standardisation Organizations (ESOs) to express them in the form of specifications in harmonised standards.

The general principle is that for the products on the market, a self-assessment of compliance with the requirements specified in Annex I will be sufficient.

For certain categories of more critical products, the application of harmonised standards will be required.

For even more critical products, a third-party assessment will be mandatory.

This report details the available standardisation outputs on the cybersecurity of products (hardware and software products, including hardware and software components of more complex products) carried out mainly by ESOs and international Standards Development Organizations (SDOs).

Specifically, the study aim at presenting a mapping of the existing cybersecurity standards against the essential requirements listed in Annex I of the CRA proposal, along with a gap analysis between the mapped standards and the requirements.

In view of the development of harmonised standards, this analysis offers a possible overview about the current coverage of the requirements by existing specifications, highlighting possible lacks that may be compensated by further standardisation work.

Upon request of DG CNECT, this study has been developed jointly by the Joint Research Centre (JRC) and the European Union Agency for Cybersecurity (ENISA).

This was also in line with the expectations of the proposal of regulation, in which it is stated that synergies on standardisation aspects should be considered between the Commission and ENISA.

In Section 2, the methodology adopted to carry out this study is summarised.

Section 3 is devoted to the presentation of the mapping between requirements and standards, giving an analysis of the coverage offered by the standards and possible gaps.

In Section 4, a summary of all identified standards and their respective mapping is offered along with some overall remarks, while Section 5 is for conclusions.

To read more:
https://www.enisa.europa.eu/publications/cyber-resilience-act-requirements-standards-mapping

Number 4

The PCAOB Will Not Tolerate Cheating

Erica Y. Williams, PCAOB Chair, Washington, DC

Public Company Accounting Oversight Board (PCAOB) Chair Erica Y. Williams made the following statement at a virtual press conference announcing the Public Company Accounting Oversight Board (PCAOB) imposed a record $25 million fine sanctioning an accounting firm, after the PCAOB found that widespread improper answer sharing occurred at the firm over a five-year period and that the firm made multiple misrepresentations to the PCAOB about its knowledge of the misconduct.

Good morning. Thank you for joining us.

Today we are announcing the largest civil money penalty in the history of the PCAOB – a $25 million fine for violations of PCAOB rules and quality control standards relating to exam cheating and misinforming investigators.

The widespread exam cheating went on for a period of five years, from 2017 to 2022, and involved hundreds of professionals, reaching as far as partners and senior firm leaders – including the firm's former Head of Assurance, who is also facing a $150,000 penalty and permanent bar under today's orders.

The growth and breadth of exam cheating in this case was enabled by the firm's failure to take appropriate steps to monitor, investigate, and identify the potential misconduct.

Furthermore, during the course of our investigation, the firm submitted – and failed to correct – multiple inaccurate representations to the PCAOB.

For example, the firm claimed to have no knowledge of answer sharing prior to a 2022 whistleblower report. Yet, this could not have been true because members of the firm's Management Board and Supervisory Board who signed off on that submission to the PCAOB had, in fact, cheated themselves.

But it doesn't end there. The accounting firm's CEO learned the submissions were inaccurate and failed to inform anyone until months later, when a second whistleblower came forward. Only then did the firm correct the inaccurate representations to investigators.

This misconduct reveals an inappropriate tone at the top and a complete failure by firm leadership to promote an ethical culture worthy of investors' trust.

I want to thank our Dutch counterparts, who conducted a parallel investigation alongside the PCAOB, for their cooperation.

The Dutch Authority for the Financial Markets has separately imposed enhanced supervision measures under Dutch law aimed at preventing recurrences.

In a global economy, the work of protecting investors does not stop at our borders. Our parallel investigations and complementary actions offer an important model for how regulators working together can strengthen accountability and ensure investors are best protected.

This case did not take place in a vacuum.

Since 2021, the PCAOB has sanctioned nine registered firms for exam cheating.

I want to be very clear: The PCAOB will not tolerate exam cheating nor any other unethical behavior, period.

Impaired ethics erode trust and threaten the investor confidence our system relies on. The PCAOB will take action to hold firms accountable when they fail to enforce a culture of honesty and integrity.

This Board set a goal to strengthen PCAOB enforcement, and we are doing just that. As of today, the PCAOB has imposed $34 million in penalties this year alone, and it's only April.

We set a record in 2022. We broke that record in 2023. And we are breaking it again today.

Let today's news be a clear warning to those who break the rules – if you put investors at risk, there will be consequences.

I want to thank our enforcement team for their continued efforts to hold firms accountable on behalf of investors.

To read more:
https://pcaobus.org/news-events/speeches/speech-detail/chair-williams-press-conference-remarks--the-pcaob-will-not-tolerate-cheating

Number 5

EIOPA publishes supervisory expectations regarding the supervision of reinsurance concluded with third-country reinsurers

European Insurance and Occupational Pensions Authority

The European Insurance and Occupational Pensions Authority (EIOPA) published today its supervisory statement on the supervision of reinsurance concluded with third-country reinsurers.

EIOPA acknowledges that reinsurance is, and should remain, an international cross-border business that leverages the global diversification of risks and offers numerous advantages to insurance undertakings. However, it is important to assess the actual risk mitigation taking place.

With this in mind, the objective of this supervisory statement is to highlight the risks stemming from the use of reinsurance provided by reinsurers operating under regulatory regimes not recognized as equivalent to Solvency II. Some parts of the statement, where relevant and explicitly stated, apply also to reinsurance arrangements with reinsurers from equivalent third countries.

To promote a high-quality and convergent supervision of such arrangements without limiting the use of reinsurance, EIOPA is proposing a risk-based approach for identifying and managing the associated risks.

The statement sets out supervisory expectations in several areas, including the assessment of the business context when using reinsurance from third countries and the importance of early supervisory dialogue.

Furthermore, it includes supervisory considerations on how to assess reinsurance agreements and undertakings' risk management systems in relation to the use of third-country reinsurers. Lastly, the supervisory statement outlines tools that would be key in mitigating any additional risks that might arise.

The statement is addressed to National Competent Authorities, which should apply it considering the principle of proportionality and following a risk-based approach.

Reinsurance is an important tool for capital and risk management used also for risks diversification, access to additional underwriting capacity for portfolio expansion, addressing protection gaps and increasing financial stability.

It plays a crucial role in the insurance industry's ability to operate and provide coverage to individuals and businesses. As such, cross-border reinsurance could offer numerous advantages to insurance undertakings.

The Solvency II Directive recognises the fact that the insurance industry is a global industry.

As such, to avoid unnecessary duplication of regulation and promote open international insurance markets, the European Commission may decide on the equivalence of a third country's (in this context non-EEA countries) solvency and prudential regime.

Particularly for reinsurance, in case of an equivalence decision according to Article 172 of the Solvency II Directive, reinsurance agreements concluded with third-country insurance or reinsurance undertakings (collectively referred to as “third-country reinsurers”) from those countries are treated in the same manner as reinsurance agreements concluded with undertakings authorised in the EU.

On the other hand, third-country reinsurers based in a non-equivalent third country may be recognized in the Basic Solvency Capital Requirement, for their own merits if their financial strength (ratings) is equal or above CQS 3 under Article 211 of the Solvency II Delegated Regulation.

Equivalence decisions are taken by the European Commission on the basis of EIOPA’s technical assessment. The list of the assessed countries can be found on EIOPA’s and European Commission’s websites.

In case of reinsurers from the United States of America (US) the EU-US Agreement on Insurance and Reinsurance (EU-US Agreement) marks an important achievement in the direction of simplifying cross-border market access.

The EU-US Agreement sets conditions to simplify EU-US market access in each other’s territory and limits group supervision of (re)insurance groups active in both territories to the level of the parent undertaking in its own jurisdiction.

Against this background, national competent authorities (NCAs) should conduct their tasks with due respect to the rights and obligations specific to each equivalence decision granted by the European Commission or any bilateral agreement between the EU and a third country, like the EU-US Agreement.

Although Solvency II includes some provisions that regulate the conditions for recognising reinsurance with third-country reinsurers, Member States may introduce national provisions, such as requiring notification, prior authorisation or the establishment of a local branch office.

The objective of this Supervisory Statement is to raise awareness of the risks stemming from regimes that have not been deemed equivalent by the European Commission and to propose a risk-based approach limiting their effect.

This Supervisory Statement is inspired by concrete cases shared by the NCAs. EIOPA intends to ensure that a highquality and convergent supervision is provided regarding insurance undertakings using reinsurance arrangements with third-country reinsurers from non-equivalent countries without limiting the use of reinsurance.

Where relevant also to reinsurance arrangements with third country reinsurers from equivalent third countries, this is explicitly mentioned in the text.

Regarding the risk profile of the reinsurance business it should be noted that differences might exist depending on whether the reinsurance arrangements are performed by reinsurance undertakings retroceding their risks (accepted from primary undertakings) or by insurance undertakings mitigating (ceding) their risks.

In fact, reinsurance undertakings have in general a business model based on the ability to write a large number of diversified risks in various markets and geographies and as such achieve a wide distribution of risks and diversification of their exposures.

Differences might also exist in the strategy, process and procedures in place regarding in particular the choice of the different reinsurance placements and how reinsurance is managed in general.

Considering these specificities, this Supervisory Statement refers mainly to insurance undertakings using reinsurance as risk-mitigation techniques; however, it might be also relevant, following a proportionate and risk-based supervision and considering the specific business models, to reinsurance undertakings retroceding their risks.

In line with EIOPA's Annual work plan 2024, EIOPA is working on the use of reinsurance including innovative reinsurance techniques and is expected to provide guidance to the NCAs in the course of 2024.

To read more:
https://www.eiopa.europa.eu/eiopa-publishes-supervisory-expectations-regarding-supervision-reinsurance-concluded-third-country-2024-04-04_en

Number 6

Chair Williams' Statement on Firm Reporting Proposal

Erica Y. Williams, PCAOB Chair, Washington, DC

For the second time today, we are taking action to bolster confidence in our capital markets, strengthen oversight and accountability, and empower investors and audit committees with consistent, comparable information.

The Firm Reporting proposal would modernize the PCAOB's framework for collecting information from audit firms by amending the annual and special reporting requirements which have not been substantively updated since 2008.

Today's proposal would facilitate the disclosure of more complete, standardized, and timely information by firms to empower investors and audit committees through greater transparency while also strengthening the PCAOB's work to protect investors.

As with the Firm and Engagement Metrics proposal, many of the proposed changes are changes that were called for in the U.S. Department of the Treasury's Advisory Committee on the Auditing Profession Report from 2008 and that have been recommended by the PCAOB's Investor Advisory Group and Standards and Emerging Issues Advisory Group.

We have also seen other jurisdictions implementing transparency reporting requirements, as well as firms voluntarily publishing some of this information on their own. Unfortunately, the voluntarily reported information is not complete or comparable.

Additionally, our staff's experience tells us that more complete, consistent, comparable information will be useful for the PCAOB's work of protecting investors.

The amendments cover five key areas:

First, Financial Information. Under the proposal, all registered firms would report actual dollar amounts of various fee categories, rather than percentages that are currently required.

The new requirements would also provide more disaggregated fee information that is more consistent and easier to compare across firms. Fee reporting would help investors, audit committees, and other stakeholders better understand how a firm's audit practice fits into its overall business and the incentives that may influence resource allocation within the firms.

The largest registered firms would also confidentially submit financial statements to the PCAOB. These firms play an essential role in our capital markets and overall economy. Their financial stability impacts their ability to invest in resources necessary to ensure quality audits and to withstand various financial events.

Second, Audit Firm Governance Information. Firms' leadership and governance have a direct impact on their incentives and ability to provide high-quality audit services investors deserve. Tone at the top and the priorities of firms' leadership strongly influence the level of commitment to audit quality.

The proposal would require all registered firms to report additional public information regarding their leadership, legal structure, ownership, and other governance information, including information on the structures and policies that would govern a change in the form of the organization.

Third, Network Information. The proposal would require a more detailed public description of firms' network arrangements, which provide an important window into the accountability and oversight structure the firm is subject to in addition to the resources the firm has available to devote to high-quality audit work.

Fourth, Special Reporting. Currently, special reporting covers certain events such as whether a firm is the subject of a lawsuit or regulatory action. The proposal would shorten the timeframe for special reporting from 30 days to 14 days or more promptly as warranted, making certain information available to investors, audit committees, and the PCAOB inspection and investigation staff in a timelier manner.

In addition to the existing special reporting requirements, the proposal would add a new confidential special reporting requirement for events material to a firm's organization, operations, liquidity or financial resources, or provision of audit services.

These events have the potential to significantly impact audit quality and investor protection, yet they are not covered under the current standard. For example, the additional requirement might include a determination that there is substantial doubt about the firm's ability to continue as a going concern; or a planned or anticipated acquisition of the firm, change in control, or restructuring.

Fifth, Cybersecurity. Cybersecurity threats are among the greatest risks to many businesses in today's world, and audit firms are particularly attractive targets.

The proposal would require public reporting of a brief description of the firm's policies and procedures, if any, to identify and manage cybersecurity risks, and confidential reporting of significant cybersecurity events to the PCAOB within five business days.

Together these provisions strengthen the PCAOB's ability to protect investors, while also providing investors with additional data to inform their own decisions and empowering audit committees with consistent data to analyze and compare as they are selecting and monitoring audit firms.

I'd like to thank the many members of the PCAOB's staff who have worked on this rulemaking project, including, from the General Counsel's Office James Cappoli, Connor Raso, Katherine Kelly, Damon Andrews, and Marc Francis; from the Office of Economic and Risk Analysis Martin Schmalz and Dylan Rassier; from the Office of the Chief Auditor Jessica Watts, Lisa Calandriello, Linnette Klinedinst, and David Ellam; from the Division of Enforcement and Investigations Kyra Armstrong, John Abell, Brett Collings, Tina Bell, and Kristin VanFossen; and from the Division of Registration and Inspections Christine Gunia, Tim Sikes, Carol Swaniker, Michael Stevenson, Alan Kerwin, Pamela Robinson, Eugene Theron, Kathleen Ostasiewski, Kevin Taylor, and Abena Glasgow.

In addition, I would like to express my gratitude to my fellow Board Members and their staff for their contributions to this project. I would also like to thank the Securities and Exchange Commission's staff, including the staff of the SEC's Office of the Chief Accountant, for their support and assistance.

I encourage all interested stakeholders to weigh in and look forward to thoroughly reviewing your comments.

To read more:
https://pcaobus.org/news-events/speeches/speech-detail/chair-williams--statement-on-firm-reporting-proposal

Number 7

Revisiting the Non-Paper

Non-Paper on EU Cyber Diplomacy, by Estonia, France, Germany, Poland, Portugal and Slovenia

Federal Foreign Office Auswärtiges Amt

Note: The german Federal Foreign Office (Auswärtige Amt) represents Germany's interests to the world. It promotes international exchange and offers protection and assistance to Germans abroad.

The Context: Changing Circumstances

Since the adoption of the Council Conclusions on Cyber Diplomacy in February 2015, several interlinked developments in the political, economic, societal and technological spheres have increased the importance of cyberspace and highlight the need for a renewed strategic reference document at EU level for cyber diplomacy:

Due to the inexorable progress of digitalisation in almost all areas of life, including in the global economy and the private lives of citizens, the need to protect the fundamental rights and freedoms of natural persons, in particular their right to privacy with regard to the processing of personal data, and the need to protect critical infrastructure in the EU and its Member States against malicious cyber-attacks are of ever-increasing importance.

Cyberspace is continuously generating novel attack targets and vectors and cyber-attacks are growing in terms of scope, frequency and sophistication as well as the damage they inflict, and state and non-state actors, including proxies, are increasingly willing to pursue their objectives by conducting malicious cyber activities varying in scope, scale, duration, intensity, complexity, sophistication and impact.

Malicious cyber activities can serve several purposes and take various forms, including attacks against infrastructure, cyber-espionage, intellectual property theft, cybercrime, and possibly also attacks in the context of hybrid threats.

The COVID-19 pandemic has demonstrated the increasing dependence on fast and stable connectivity and that a functioning, stable and secure cyberspace is an important condition for this.

Cyberspace has increasingly become an area of strategic competition between states which reflects the dynamic geopolitical environment in recent years, and technological innovations have increasingly become points of contention between states due to their growing significance for economic and military competitiveness, which has also resulted in a technological confrontation between major actors.

More confrontational approaches in the technological realm may lead to certain decoupling effects and to a further severing of global supply chains and cooperation with regard to research and innovation, including in the area of cyber security, as well as to a potential fracturing of the global internet, which is noted with concern.

The EU and its Member States have to clearly define their role in the context of growing competition between major actors that are increasingly willing to shape the digital environment and the discussion surrounding it, meaning that the EU and its Member States have to assert themselves in international cyberspace norm-setting and technological standard-setting bodies.

States with an authoritarian outlook are increasingly trying to enforce their interests in cyberspace and in the technological realm and the EU and its Member States have to react by promoting their values and interests, which include human rights, prosperity, security and Europe´s digital sovereignty.

The use and deployment of technologies to track, surveil, anticipate or even grade the behaviour of citizens in a repressive and unprecedented way, and the use of digital tools by authoritarian states that is contrary to the idea of a free, open and global internet and international human rights law as well as plans by some countries to build an alternative internet regulated by the State are noted with concern.

Protection of its Citizens and Modern Societies

Recent EU cyber-related initiatives aimed at protecting its citizens and the resilience of its modern societies and the related data and critical infrastructure against malicious activities in cyberspace, such as the renewed Cyber Security Strategy, Review of the NIS Directive and the EU 5G Toolbox with its objective of establishing a coordinated European approach aimed at mitigating the main cyber security risks of 5G networks, are welcomed and the importance of maintaining and strengthening coherence among the EU cyber and digital initiatives is noted.

With the advent of innovative technologies such as artificial intelligence, the Internet of Things or 5G, new possible targets and vectors are emerging in cyberspace, which also have to be reflected in global debates concerning norms of behaviour in cyberspace.

Furthermore, cybercrime actors are steadily developing new forms of malicious activities to exploit vulnerabilities in cyberspace.

While digital technologies and increased connectivity are key components of modern societies and bring major benefits in terms of growth and prosperity, at the same time citizens, companies and governments are, especially in the context of the COVID-19 pandemic, more and more exposed to offenses in the field of cybercrime, which are steadily increasing in number and sophistication.

Thus, the EU and its Member States reiterate the need for a coordinated and determined fight against cybercrime and continue to promote the Council of Europe Convention on Cybercrime, also known as the Budapest Convention, and the negotiations on the Second Additional Protocol to the Budapest Convention, as an important framework for international cooperation in the fight against cybercrime.

Regarding access to digital evidence, the EU and its Member States first recognize encryption as an important tool for the protection of cybersecurity and fundamental rights, such as privacy, including the confidentiality of communications, and personal data.

The EU and its Member States are invited to find solutions that allow law enforcement and other competent authorities to gain lawful access to digital evidence concerning malicious cyber activities, without prohibiting or generally weakening encryption, and in full respect of privacy and fair trial guarantees consistent with applicable law.

The EU and its Member States acknowledge in that context the work done by EUROPOL and similar European and international institutions with a view to supporting and coordinating investigations of cyber-attacks and cybercrime among the Member States.

The EU, for instance in the context of the Horizon Europe framework programme, and its Member States are encouraged to further invest in cyber security research, including in the areas of digital forensics analysis, threat intelligence and incident response in the face of malicious activities in cyberspace.

Cyberspace as a Key Area for the EU's Foreign Policy and Digital Sovereignty

Due to the increasing importance of cyberspace for several areas of life and the growing significance of digital technologies for power projection on the international stage, cyber diplomacy should be considered an important tool for fulfilling the objectives and interests of the EU.

The protection and reinforcement of Europe's digital sovereignty in the EU stands in direct connection with cyber security, as it ensures trust in digital technologies and the digital transformation process.

Thus, a coherent international cyberspace policy must be considered a key component of the determined engagement of the EU and its Member States with a view to reinforcing their digital sovereignty by having the ability and the will to shape global debates, which reflects the EU's values as well as its strategic and economic interests, and the capacity to act selfassertively in cyberspace, which should not be confused with isolating itself or striving for digital or technological autarky.

Through its engagement – within the EU and beyond – with regard to setting norms of behaviour and establishing regulations concerning cyberspace and its self-conception as a preventive actor in contributing to a secure, stable and open cyberspace, the EU serves as an international point of reference, especially for states which want to avoid confrontational approaches internationally and adhere to international law in cyberspace, and the EU positions itself as a champion of and force for peaceful relations, conflict prevention and greater stability in cyberspace.

The EU with its human-centred approach is in an excellent position to set sophisticated cyber-related and technology standards, such as the General Data Protection Regulation (GDPR) or the ethical and legal framework proposed by the AI White Paper concerning high-risk applications, which serves as a model for other regions.

Such a coherent international cyberspace policy of the EU – especially in the context of the previously mentioned numerous and interlinked developments in the political, economic, societal and technological spheres – should serve:

• the EU's foreign and security policy objectives and broader values, as stated in the EU Global Strategy, with cyber diplomacy being an integral part of the pursuit of these goals in the context of the Common Foreign and Security Policy (CFSP), and with activities in cyberspace being conceived jointly and in line with contextual developments at international level;

• the purpose of protection of its citizens and modern societies, and of the related data and critical infrastructures, against malicious activities in cyberspace, as well as the integrity and security of the EU and

• the purpose of promotion and protection of the fundamental EU values of democracy, human rights, gender and digital equality and the rule of law in cyberspace, including the right of expression and equal access to and secure use of information and communication technology (ICT) and the internet, on the global stage, especially in light of the increasing misuse of new technologies that leads to human rights and privacy violations.

EU Cyber Diplomacy Toolbox

The added value of the Cyber Diplomacy Toolbox, introduced by the Conclusions on the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities, which in a transparent and resolute way provides the EU and its Member States with instruments to give adequate and determined responses to malicious cyber activities with a wide range of diplomatic, political and economic measures, is strongly welcomed. The Toolbox comprises:

(i) Preventive Measures,
(ii) Cooperative Measures,
(iii) Stability Measures,
(iv) Restrictive Measures and
(v) Possible EU support to Member States' lawful responses.

To read more:
https://www.auswaertiges-amt.de/blob/2418160/206b3bf9aa4ef45a288739923
1840d23/201119-non-paper-pdf-data.pdf

Number 8

CISA Issues Emergency Directive 24-02: Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System

CISA issued Emergency Directive (ED) 24-02 to address the recent campaign by Russian state-sponsored cyber actor Midnight Blizzard to exfiltrate email correspondence of Federal Civilian Executive Branch (FCEB) agencies through a successful compromise of Microsoft corporate email accounts.

This Directive requires agencies to analyze the content of exfiltrated emails, reset compromised credentials, and take additional steps to secure privileged Microsoft Azure accounts.

While ED 24-02 requirements only apply to FCEB agencies, other organizations may also have been impacted by the exfiltration of Microsoft corporate email and are encouraged to contact their respective Microsoft account team for any additional questions or follow up.

All organizations are strongly encouraged to apply stringent security measures, including strong passwords, multifactor authentication (MFA) and prohibited sharing of unprotected sensitive information via unsecure channels.

To read more:
https://www.cisa.gov/news-events/alerts/2024/04/11/cisa-issues-emergency-directive-24-02-mitigating-significant-risk-nation-state-compromise-microsoft

Number 9

Listening to the Data: How a NIST Tool Helps Labs Worldwide Harmonize Measurements

If a traveler from Germany goes to Vietnam and falls ill, the results of their blood test there should be as meaningful as if the test were taken at home. If a Japanese airliner lands in Argentina and needs a part, that part needs to be installed using properly calibrated tools.

Commerce, science, engineering, medicine and most other human activities depend on measurements. In a global economy, measurements need to be reliably comparable across the world.

But how do we ensure that actually happens?

National metrology institutes — NIST and equivalent institutes in other countries — participate often in rigorous, challenging comparisons of their measurement capabilities.

Each laboratory measures the same material or piece of equipment, generally following the same steps, and then the labs compare results. These are called key comparisons. If the results are not mutually consistent, then it's a learning opportunity for the participants to improve their measurement procedures.

Agreeing to the Rules

The question for researchers is how best to combine everyone's results into a consensus value. Let's say we're measuring the concentration of lead in wine.

The participating labs receive vials of wine and measure them according to a specified protocol. Ideally, the consensus value for the concentration of lead in the wine is expected to be closer to the truth than individual measurements are.

Although it doesn't always work out that way, that's the goal of these types of studies.

The measurement results that are combined into a consensus value each include a measured value (how much we think there is of whatever is being measured) and an evaluation of the measurement uncertainty.

Because measurements aren't perfect, measurement uncertainty is the doubt that remains about the true value of a quantity after making a measurement; it's the "give or take" margin.

Uncertainty is like fog. If you're driving and there's a little fog, you may be on higher alert to your surroundings to make sure you can drive safely. But if there's so much fog you can barely see, your drive is much more dangerous. Uncertainty is like a fog that surrounds the true value you are after. The greater the uncertainty, the greater the doubt about what the truth really is.

So, if I asked you to determine the mass of the beans in a bag of coffee beans, you might reach the conclusion that it is 1,000 grams, give or take 15 grams.

The 1,000 grams is how much we measured, and the 15 grams is the measurement uncertainty. This means that the true mass of the coffee beans is likely to be between 985 grams and 1,015 grams.

The obvious answer to the question of how to come up with a consensus value may be to average the measured values from the different labs.

But this isn't necessarily the best answer because different measurement results may have different uncertainties, and some measurement results may be very far from most of the others.

Outlying measurements often call for reexamination and may require special treatment.

Very often, participating labs disagree on how best to blend the results from a key comparison into a consensus value. They also sometimes don't agree on how the individual results should be compared with the consensus value and with one another.

Such disagreement can create considerable difficulties and delays. Imagine a sport where before every game, the participants had to negotiate the rules! It's unwieldy.

That's why NIST statisticians and scientists created a web-based tool called the NIST Decision Tree. Organizers of an interlaboratory study can use the tool to determine how to best handle the study's data.

The tool offers suggestions, but the scientists are always in the driver's seat to choose the data analysis procedure that they believe fits their data and best serves the purpose of their study.

The tool asks researchers a few simple questions about their data. Based on the answers, the NIST Decision Tree makes a recommendation for how that data should be modeled and analyzed. To go back to the sports analogy, we suggest rules for the participants in the game to agree to.

Real-World Uses for the NIST Decision Tree

Let's say we're doing a study where different laboratories measure how much arsenic there is in a sample of rice flour. That's a measurement that we need to get right because of the stakes for people's health.

A laboratory leading a study would prepare a batch of the flour, fill vials with it, seal the vials and ship them to participants. Before they are shipped, the organizing laboratory would run its own preliminary study to verify that the samples of flour in the vials have essentially the same amount of arsenic. The lab would measure how many micrograms of arsenic per gram of flour, for example.

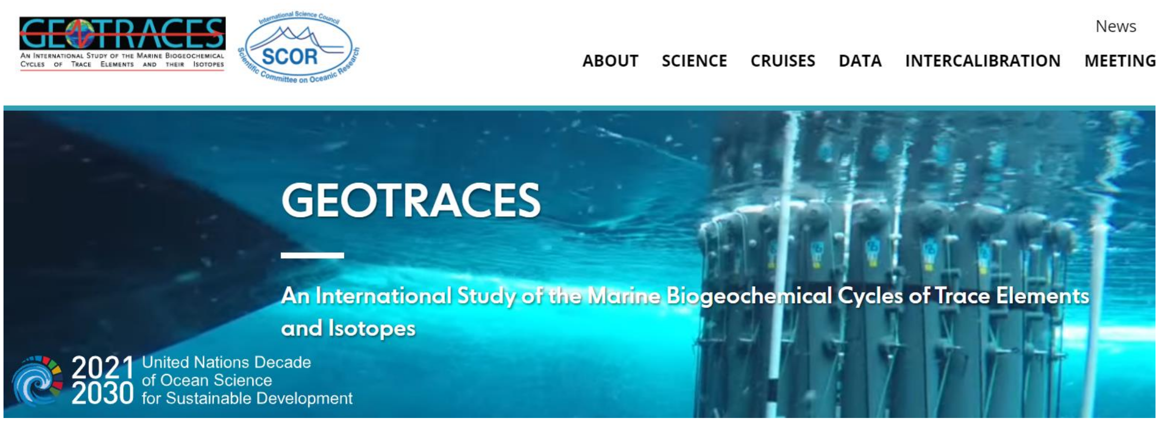
The labs participating in the study would receive a protocol on how to handle the flour and, possibly, suggested measurement steps to determine the amount of arsenic in it. In other cases, the participating labs choose their own measurement methods.

Once the measurements have been completed, the labs have to agree on how their measurement results will be compared. This is often a contentious topic that takes time and resources. That's where the NIST Decision Tree comes in.

A key part of this process is selecting the best statistical model to use to analyze the data. I call such identification "listening to the data." A good statistical model should be respectful of the data and of the people who have meticulously planned and conducted experiments to obtain it.

The NIST Decision Tree has been used in quite a few studies so far, including in key comparisons in chemistry and in temperature measurements organized by subcommittees of the International Committee for Weights and Measures.

We're now working with oceanographers to determine how the NIST Decision Tree can be used in an international cooperative effort to study changing ocean and environmental conditions, known as GEOTRACES.



To read more:
https://www.nist.gov/blogs/taking-measure/listening-data-how-nist-tool-helps-labs-worldwide-harmonize-measurements

Number 10

Lawrence Livermore National Laboratory (LLNL) - See the solar corona: an intricate pattern reveals itself during the April 8 eclipse

On Monday, April 8, a swath of North America will experience a total solar eclipse. For a few minutes, the moon will completely obscure the sun and viewers will be able to see the intricate loops and flares in the solar corona—normally washed out by the bright disk of the sun.

In the corona, the outermost, gaseous part of the sun's atmosphere, particles dance around invisible magnetic field lines to make complex structures.

Imagine the particles like cars racing through a city, merging onto highways and roundabouts, turning onto side streets and stopping at traffic lights.

But the magnetic field "roads" in the corona are invisible, creating a beautiful, chaotic, hard-to-decipher pattern of particles.

Since the 1980s, researchers at Lawrence Livermore National Laboratory (LLNL) have been unraveling the patterns in the solar corona using a device called an electron beam ion trap (EBIT).

"In astronomical objects like the Sun, there are a lot of things going on at the same time. You have emission from all these different ions and atoms," said Alex Fairchild, a postdoctoral researcher at LLNL. "In the laboratory setting we can disentangle processes that occur simultaneously in the corona. We can measure and identify emission from a single ion species."

To accomplish this, Fairchild and his collaborators use a series of electric and magnetic fields to create a dense stream of electrons and aim it at target atoms like silicon or iron. The resultant collisions ionize and excite the atoms, which release their extra energy in the form of ultraviolet (UV) and X-ray light.

By examining the emission, LLNL scientists can test models of the sun and help interpret solar observations. They use this information to assist solar physicists with determining the temperature and density of the solar corona.

Understanding the solar corona becomes crucial as the number of satellites in space increases. Flares and solar wind material ejected from the sun's atmosphere affect space weather, which can interfere with satellites and GPS.

There's also a long-standing fundamental physics problem: coronal heating.

"The sun's corona is actually much hotter than its surface, which is a bit counterintuitive," said Fairchild. "This is like if a light bulb raised the temperature of the surrounding air to a temperature much hotter than the light bulb itself. We don't completely understand how the solar atmosphere at higher elevations, where we expect it to be colder, is so hot."

"If you're interested in this kind of work, LLNL is one of the best places to be," said Fairchild.

LLNL's EBIT-I and SuperEBIT electron beam ion traps have been used for over three decades to help answer questions related to solar physics, astrophysics, and fusion science.

Find more information here about LLNL's EBIT laboratory astrophysics work: https://space-science.llnl.gov/research/x-ray-and-laboratory-astrophysics

The eclipse's path of totality begins in Mexico, and the path of totality will pass through Texas, Oklahoma, Arkansas, Missouri, Illinois, Kentucky, Indiana, Ohio, Pennsylvania, New York, Vermont, New Hampshire and Maine. Those outside the path of totality can still catch a partial solar eclipse. Anyone looking at the sun should use proper safety glasses.

To read more:
https://www.llnl.gov/article/51101/see-solar-corona-intricate-pattern-reveals-itself-during-april-8-eclipse

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.

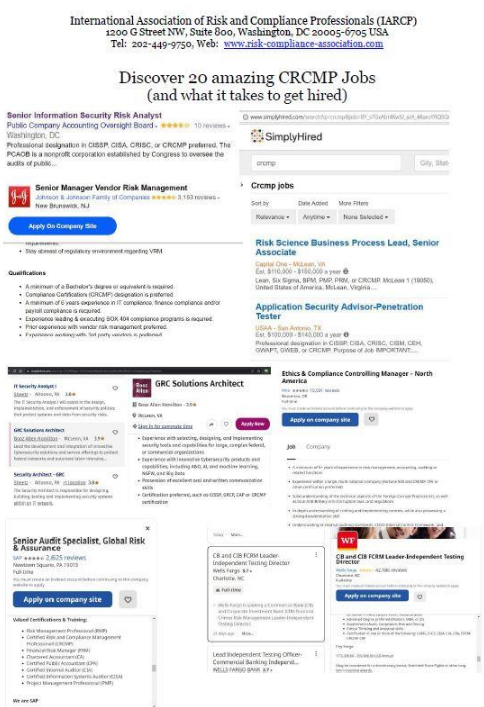
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

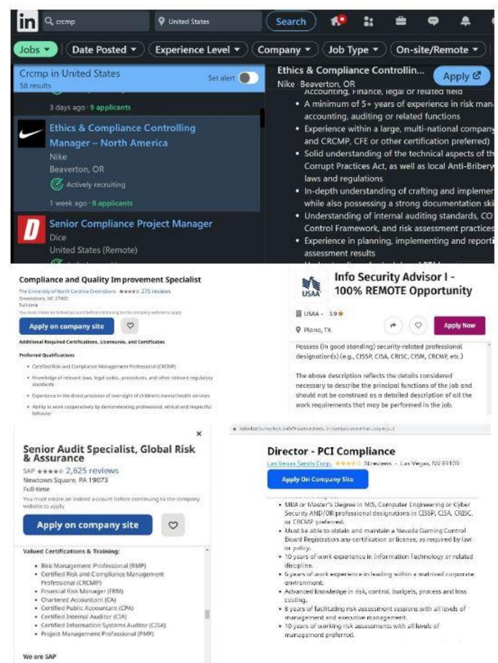
Our training and certification programs:

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