International Association of Risk and Compliance Professionals (IARCP)
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA
Tel: 202-449-9750, Web: www.risk-compliance-association.com

Monday, October 24, 2022

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

Dear members and friends,

"Mirror, mirror on the wall, who in this land is fairest of all?"

Children's fiction can open up new perspectives for adults. Black swan events, exercising (or failing to exercise) the zero-trust principle, risks and opportunities are all there.

Investigating the narrative is the next step. In 1994, Eckhard Sander claimed that the character of *Snow White* was based on the life of Margaretha von Waldeck, a German countess born in 1533. At the age of 16, Margaretha was forced by her stepmother, Katharina of Hatzfeld, to move away to Brussels. There, Margaretha fell in love with a prince who would later become Philip II of Spain.

Graham Anderson compares the story of Snow White to the Roman legend of Chione, recorded in Ovid's Metamorphoses. Chione means "snow" in

Greek, and, in the story, she is described as the most beautiful woman in the land, so beautiful that the gods Apollo and Hermes both fell in love with her.

For Snow White, the death of her real mother and the arrival of a stepmother is a disaster. Snow White is forced to leave home, but she discovers who she is, and moves along the path to self-discovery and resilience. This is a story about developments set in motion by the arrival of evil. Does it look familiar?

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

Number 1 (Page 5)

EIOPA sets out its strategy for 2023 – 2026

Number 2 (Page 7)

Proposed Articles of the European Cyber Resilience Act

Number 3 (Page 10)

Request for Information and Comment
The Application and Use of the PCAOB's Interim Attestation Standards

Number 4 (Page 13)

EBA publishes its work programme for 2023

Number 5 (Page 15)

Mask Gate as a Continuous Media Event in a Hybrid Media Space

Number 6 (Page 20)

EIOPA, Revised Single Programming Document 2023-2025
Including Annual Work Programme 2023

Number 7 (Page 24)

Federal Reserve Board announces that six of the largest banks will participate in a pilot climate scenario analysis exercise

Number 8 (Page 26)

Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization

Number 9 (Page 28)

BINDING OPERATIONAL DIRECTIVE 23-01

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Number 10 (Page 36)

Scientists chip away at a metallic mystery, one atom at a time

It's no secret that radiation weakens metal. Uncovering how is complicated work.

Sandia National Laboratories

Number 1

EIOPA sets out its strategy for 2023 – 2026

The European Insurance and Occupational Pensions Authority (EIOPA) has set out its strategy for the period 2023 – 2026.

Current geopolitical tensions due to Russia's unprovoked invasion of Ukraine coupled with lingering effects of the pandemic, market volatility and inflation underline the need for effective supervision.

Building on a strong foundation, the strategy is designed to strengthen the resilience and sustainability of the insurance and pensions sectors, and to ensure the strong and consistent protection of consumer interests across the European Union.

Under the overall vision of building a safe and sustainable EU for citizens in times of transformation, EIOPA has identified strategic priorities on which to focus.

- Sustainable finance. Contribute to building up sustainable insurance and pensions, including by addressing protection gaps, for the benefit of citizens and businesses.

- Digital transformation. Support the supervisory community and industry to mitigate the risks and seize the opportunities of the digital transformation, including by further promoting a data-driven culture.

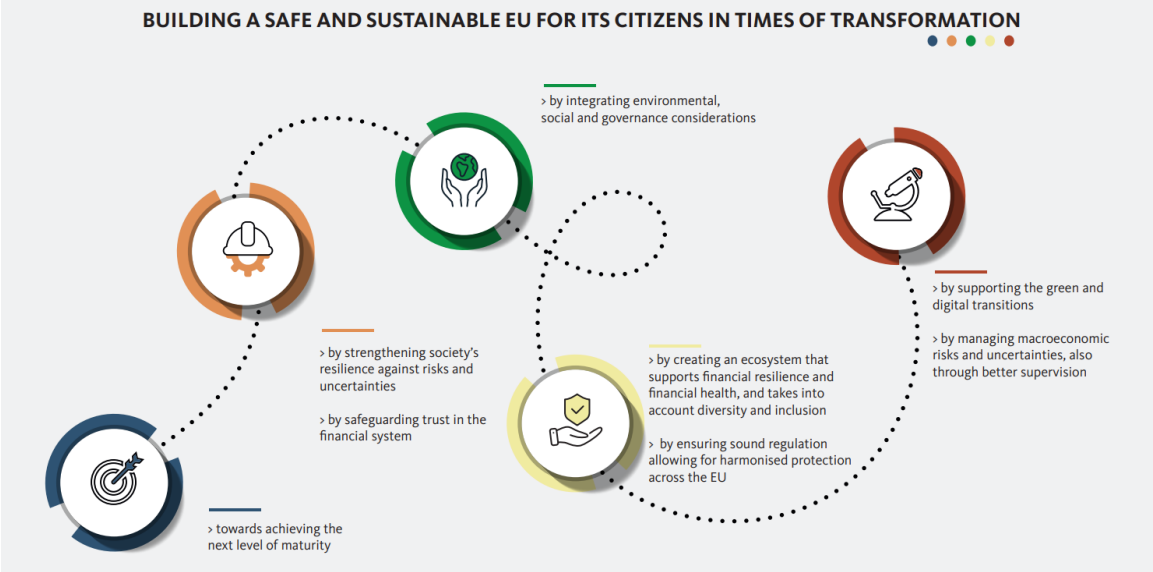
- Supervision. Promote sound, efficient and consistent prudential and conduct supervision throughout Europe, particularly in view of increased cross-border business.

- Policy. Deliver high-quality advice and other policy work taking into account changing and growing needs of society as well as the effects of new horizontal regulation.

- Financial stability. Further enhance financial stability, with particular focus on the analysis of financial sector risks, vulnerabilities, and emerging threats.

- Internal governance. Be a model EU Authority with high professional standards, cost-effective governance, and a positive reputation within the EU and globally.

To fulfil its objectives, EIOPA will continue to work in a collaborative and consultative way, valuing the guidance of its Board of Supervisors, and the input from a range of stakeholders.



The strategy:
https://www.eiopa.europa.eu/sites/default/files/publications/administrative/eiopa-strategy-2023-2026.pdf

Number 2

Proposed Articles of the European Cyber Resilience Act

The proposal for a regulation on cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act, bolsters cybersecurity rules to ensure more secure hardware and software products.

Hardware and software products are increasingly subject to successful cyberattacks, leading to an estimated global annual cost of cybercrime of €5.5 trillion by 2021.

Such products suffer from two major problems adding costs for users and the society:

- a low level of cybersecurity, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and

- an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.

While existing internal market legislation applies to certain products with digital elements, most of the hardware and software products are currently not covered by any EU legislation tackling their cybersecurity.

In particular, the current EU legal framework does not address the cybersecurity of non-embedded software, even if cybersecurity attacks increasingly target vulnerabilities in these products, causing significant societal and economic costs.

Two main objectives were identified aiming to ensure the proper functioning of the internal market:

- create conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and ensure that manufacturers take security seriously throughout a product's life cycle; and

- create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements.

Four specific objectives were set out:

1. Ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole life cycle;

2. Ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers;

3. Enhance the transparency of security properties of products with digital elements, and

4. Enable businesses and consumers to use products with digital elements securely.

For the purposes of this Regulation, the *following definitions* apply:

'Product with digital elements' means any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately;

'Remote data processing' means any data processing at a distance for which the software is designed and developed by the manufacturer or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions;

'Economic operator' means the manufacturer, the authorised representative, the importer, the distributor, or any other natural or legal person who is subject to obligations laid down by this Regulation;

'Manufacturer' means any natural or legal person who develops or manufactures products with digital elements or has products with digital elements designed, developed or manufactured, and markets them under his or her name or trademark, whether for payment or free of charge;

'Authorised representative' means any natural or legal person established within the Union who has received a written mandate from a manufacturer to act on his or her behalf in relation to specified tasks;

'Importer' means any natural or legal person established in the Union who places on the market a product with digital elements that bears the name or trademark of a natural or legal person established outside the Union;

'Distributor' means any natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a product with digital elements available on the Union market without affecting its properties;

'Software' means the part of an electronic information system which consists of computer code;

'Hardware' means a physical electronic information system, or parts thereof capable of processing, storing or transmitting of digital data;

'Significant cybersecurity risk' means a cybersecurity risk which, based on its technical characteristics, can be assumed to have a high likelihood of an incident that could lead to a severe negative impact, including by causing considerable material or non-material loss or disruption;

Our strategic partner, Cyber Risk GmbH, is carefully monitoring the developments. You may visit:
https://www.european-cyber-resilience-act.com

This is a difficult compliance challenge, as "the Regulation applies to products with digital elements, whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network."

Number 3

Request for Information and Comment

The Application and Use of the PCAOB's Interim Attestation Standards

PCAOB
PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD

The staff of the Public Company Accounting Oversight Board is requesting information and public comment on matters related to the application and use of the Board's interim attestation standards.

In April 2003, the Board adopted on an interim basis certain attestation standards from the American Institute of Certified Public Accountants. These standards have continued in effect substantially as they were adopted.

The Board is committed to modernizing its standards, and this document requests information and comment from the public to inform any staff recommendation to the Board regarding updates to the interim attestation standards, including possible consolidation or elimination of certain standards.

The PCAOB is committed to modernizing its existing standards and to issuing new standards where necessary in light of developments in auditing and the capital markets. In that regard, the Board is considering updating its interim standards1 related to attest engagements ("PCAOB attestation standards").

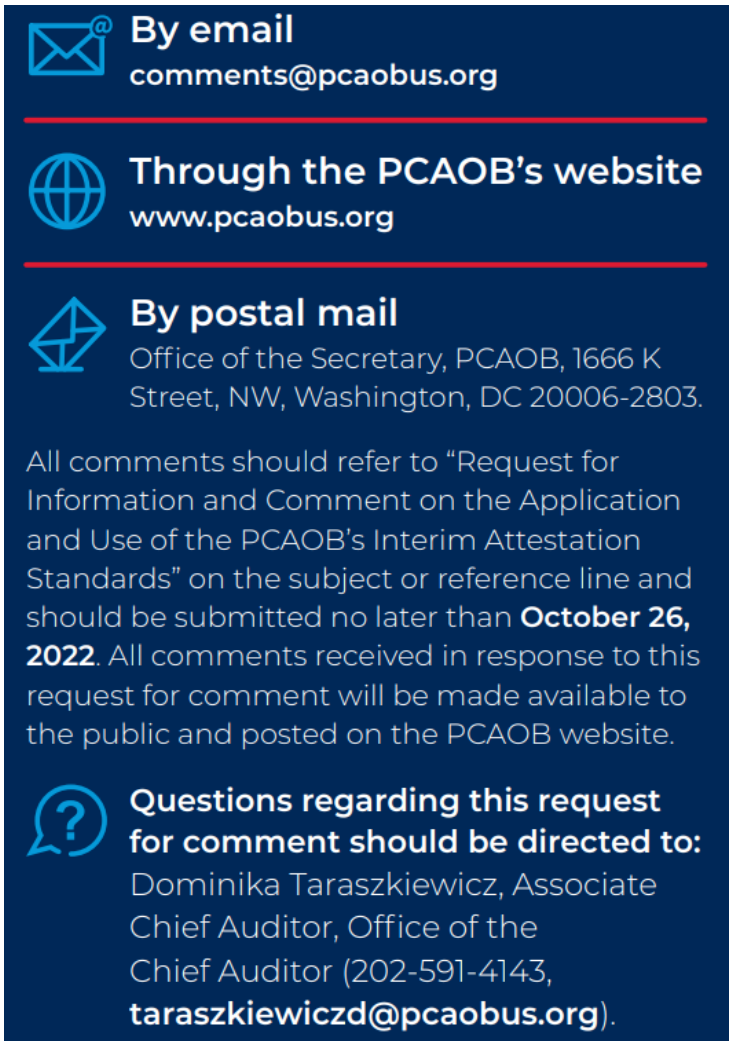
Registered public accounting firms are sometimes engaged to examine and report on matters outside of an audit of financial statements.

These engagements include examination, review, and agreed-upon procedures engagements, which involve issuing a report on subject matter, or an assertion about subject matter, that is the responsibility of another party ("attest engagements").

The subject matter of an attest engagement can vary and may relate to, for example, a company's compliance with laws and regulations, or a company's historical data or measures that are evaluated against certain criteria.

An attest engagement performed under PCAOB standards is designed to provide a certain level of assurance (as described below) and involves issuing a corresponding report ("attestation report"):

- Examination attest engagements provide reasonable assurance;
- Review attest engagements provide moderate assurance; and
- Agreed-upon procedures attest engagements do not provide specific assurance but involve a report on the performance of specified procedures and the resulting findings.



To read more:
https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/standards/staff-request-for-comment/rfc-application-use-interim-attestation-standards.pdf?sfvrsn=fd791256_2

Number 4

EBA publishes its work programme for 2023

The European Banking Authority (EBA) published today its annual work programme for 2023, describing the key strategic areas of work for the Authority for the coming year, as well as related activities and tasks.

In 2023, the EBA will continue delivering on the priorities defined for the period 2022-2024 in its programming document.

Its focus will be on:

i) finalising the Basel implementation in the EU,

ii) running an enhanced EU-wide stress test,

iii) providing data to all stakeholders,

iv) addressing the new challenges arising from the digitalisation of finance, and

v) further contributing to the build-up of the capacity to fight ML/FT and to protect consumers in the EU.

Moreover, it will continue to pay particular attention to the European ESG agenda, in its regulatory and risk assessment mandates, as well as in its own organisation, building on its recent EU Eco-Management and Audit Scheme (EMAS) registration.

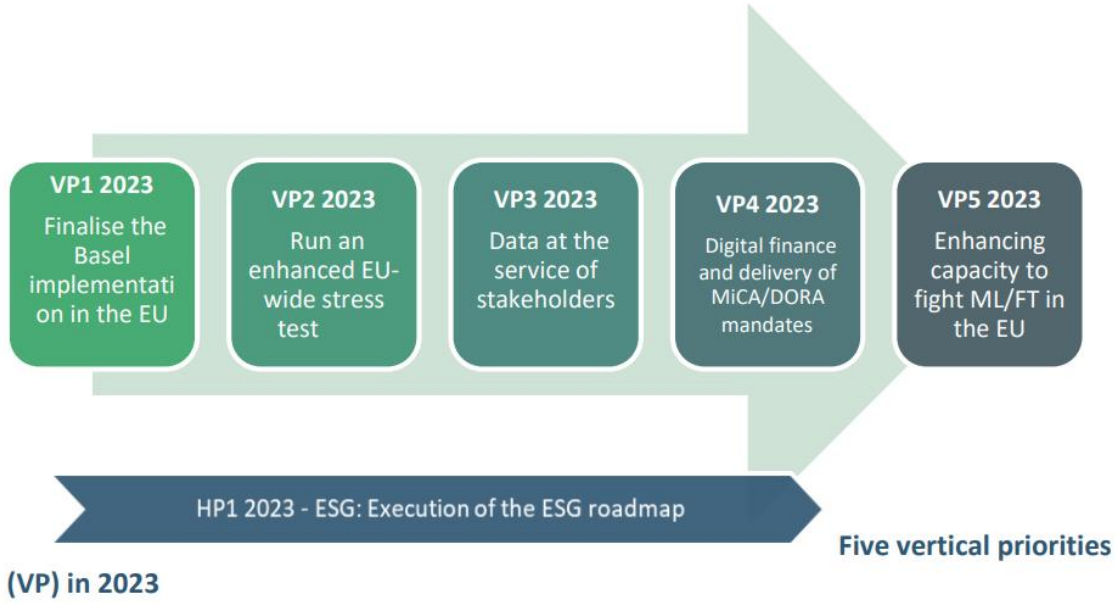
Given the political agreements reached in 2022 on the Digital Operational Resilience Act (DORA) and Markets in Crypto-Assets (MiCA) legislations, the EBA will also actively start its preparations to be able to discharge the new oversight responsibilities it will receive, together with the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA).

Against this background, it will continue to foster all possible internal and external synergies, working closely with Competent Authorities and other European bodies, and carry out the modernisation of its organisation engaged in recent years.

Against that background, the number of over-arching activities was further reduced to facilitate coordination and readability.

The work programme benefitted from the recommendations of the EBA's Advisory Committee on Proportionality.

The executive summary of the EBA work programme for 2023 will be made available in all EU official languages.



To read more:
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2022/1039834/2023%20EBA%20Work%20Programme.pdf

Number 5

Mask Gate as a Continuous Media Event in a Hybrid Media Space

This study examines the evolution of the "Mask Gate" media event that took place in Finland amidst the COVID-19 pandemic and state of emergency in 2020.

In March-August 2020, there was a dispute between various public health institutions and authorities as to whether the public should be required to use face masks.

This investigation focuses on the construction of the media event, specifically on the interplay and dynamics between social media and mass media, as well as the public reactions evoked by the Mask Gate in Finland.

Our aim is to describe the critical turning points in the development of the media event, thus tracing the evolution of such media events in the present media system.

We illustrate our case with the help of a data set consisting of 391 033 messages about respiratory masks found on social media and traditional news media outlets.

We focus our analysis on a subset of this data set concerning the "Mask Gate". On the basis of our analysis, we present a timeline of the Mask Gate as well as analyse the most important actors, platforms and affective reactions that played a role in the construction of the event.

An autopsy of such a notable media event can assist organisations in developing their communication competencies for risk, strategic and crisis communication situations, in which it is imperative for an organisation to restore its public legitimacy.

Introduction

On April 8th 2020, Finnish weekly Suomen Kuvalehti had a scoop claiming that the Finnish National Emergency Supply Agency had purchased face masks via two Finnish agents worth a combined 10 million euros (Liski, 2020).

The procured Chinese masks appeared to be unsuitable for hospital use due to their low quality. According to the report, partners of the deal were a businessman who ran a quick-loans company before running heavily into debt, a beauty-sector entrepreneur and a convicted white-collar criminal (Yle News, 2020).

Due to the public outcry regarding this failed deal, the Finnish government accepted the resignation of the head of the Finnish National Emergency Supply Agency.

The failed face mask deal raised questions about the organisation's competence and resilience, igniting a public legitimacy crisis for the respective institutions.

Later on in October of 2020, opposition politicians accused the government of providing misleading information concerning the effectiveness of masks in the spring, when the Prime Minister said that the shortage of masks was one of the reasons for not giving a large-scale recommendation for using masks (Vaarala & Koivuranta, 2020).

This event reinvigorated the debate and Mask Gate reappeared in the media. Thus, the failed deal can be conceived of as only as the starting point for an extensive public debate and political struggle that revolved around the subject of masks.

This study is aimed at unpacking and analysing the construction of the media event, specifically on the interplay and dynamics between social media and mass media and the public reactions evoked by Mask Gate in Finland.

Our aim is to describe the important turning points along the emergence and development of this media event. By understanding the construction of a media event in a hybrid media space, we can learn more about how such media events may influence the public understanding and interpretation of the events.

This is especially important in times of societal crises, when the sense of psychological security is at stake, necessitating access to the best evidence-based information.

The motivation for studying this debate is twofold:

First, it is important to understand how such a media event evolved in the current media system. Mask gate was caused because of apparent failures in the face mask acquisition process, and the ensuing political debate

concerning the accusations of misleading information can be seen as the aftermath and next phase of the mask acquisition scandal.

An autopsy of such a huge media event can assist organisations in developing their communication competencies for risk and crisis communication situations, in which it is imperative for an organisation to restore its public legitimacy and curb mis- and disinformation.

Moreover, we focus on the role of mediated emotions in driving the event and discussion. It is important to understand how mediated emotions, such as "moral panics", can escalate and how the sense of psychological security can be distorted (e.g. Kellner 2003; Cottle 2006, Döveling, Harju & Sommer, 2018).

Second, we need more knowledge on the role of social media and the interplay of social and traditional media in the digital sphere. We have significant data points available through media monitoring systems on media events, but we remain limited in our understanding of their social construction and the role of public audiences in this process.

This remains the case, even though these events have a major impact on our society through their ability to adjust opinions, diffuse information widely, and influence people's mood and perceptions, as well as trust in public institutions critical for the functioning and integrity of democratic systems.

Date	Event
March 13. 2020	The Government and the President declared that Finland is in a state of emergency due to the COVID-19 pandemic and decided to adopt the Emergency Powers Act.
April 3. 2020	Finnish Institute of Occupational Health and FIMEA claimed that "Self-made masks do not protect against the virus, and at worst cause harm."
April 14. 2020	Message from the CEO of the Finnish Institute for Health and Welfare: Wear a cloth mask in public places.
April 14. 2020	Ministry of Social affairs and Health claim that they "do not provide a mask recommendation."
May 5. 2020	The Finnish Broadcasting Company: "Face masks mandatory in more than 50 countries - why not in Finland?"
May 5. 2020	Ministry of Social affairs and Health's Chief of Staff in A-Studio: "We will find out the benefits of masks."
May 14. 2020	Technical Research Centre of Finland: "The fabric mask may protect others, but not the user."

Date	Event
May 22. 2020	The Finnish Broadcasting Company: Opposition to support the mask recommendation.
May 29. 2020	Ministry of Social affairs and Health's report explains: The benefits of masks in everyday life are small or non-existent.
June 2. 2020	The government's science panel disagrees - recommends the use of face masks in its report.
June 3. 2020	Minister Krista Kiuru: There is no general mask recommendation from the government, but a protector can be used to protect others
July 31. 2020	A new, external study of Ministry of Social affairs and Health's data: Masks do bring health benefits.
Aug 13. 2020	Finnish Institute for Health and Welfare: Mask recommendation for almost the whole country; PM Marin announces government support.
Sep 24. 2020	The Face Mask recommendation is updated.
Oct 8. 2020	PM Marin says at a government question and answer session that a mask recommendation was not issued in the spring because there were not enough masks available.
Oct 9. 2020	Minister Kiuru defends the government's recommendations in the spring by "the uncertainty of the situation".
Oct 11. 2020	PM Marin tweets about Mask Gate and denies allegations of lying and misleading the Finnish people.
Oct 12–14. 2020	Intensive public debate between Finnish Institute for Health and Welfare and Ministry of Social affairs and Health, both on traditional and social media.
Oct. 15. 2020	PM Marin reports to the media that the debate is now closed.

- **Actors. There are multiple** actors who create the event in the current media environment. They can be human or non-human (Latour 2005). Human actors can be individuals or a collective. Non-human actors are platforms, algorithms, AI, etc. In traditional media events, the central role was played by journalistic mainstream media, politicians and officials. Now anyone (an individual or collective) can influence the media event by mass communication (Castell 2009). These different actors are interconnected and networked by the hybrid media system.

To read more:
https://stratcomcoe.org/publications/mask-gate-as-a-continuous-media-event-in-a-hybrid-media-space/248

Number 6

EIOPA, Revised Single Programming Document 2023-2025

Including Annual Work Programme 2023

Foreword 3

EIOPA's Mission and vision 5

Acronyms 6

Section I: General context 7

Section II: Multi-annual programme 2023-2025 11

Key Performance Indicators 2023-2025: 12

1. Human and Financial Resources Outlook 16

1.1. Overview of the past and current situation 16

1.2. Workload outlook for 2023-2025 17

1.3. Resource Programming for 2023-2025 21

1.4. Strategy for Achieving Efficiency Gains 22

1.5. Negative Priorities 25

Section III: Annual Work Programme 2023 28

Operational Priorities 28

Annual Activities 2023 30

Annexes 67

I. Organisational Chart – December 2021 68

II. Resource Allocation per Activity 69

III. Financial Resources 70

IV. Human Resources – Quantitative 77

V. Human Resources – Qualitative 83

VI. Environmental Management 91

VII. Building Policy 92

VIII. Privileges and Immunities 94

IX. Evaluations 95

X. Organisational Management and Internal Control 96

XI. Plan for Grant, Contribution or Service- Level Agreements 98

XII. Cooperation with third States and International Organisations 100

In a context characterised by evolving challenges, risks and opportunities EIOPA will focus on managing the uncertainty in times of transformation to ensure robust insurance and pensions sectors in Europe.

The Russian invasion has provoked a humanitarian crisis, a political crisis and an economic crisis. One that not only is urgent now, but that will also impact many economic and political decisions in the future.

In 2022, we have been observing an abrupt change in the economic and financial situation. Supply chain disruptions, spiking energy and commodity prices triggered by the prolonged pandemic crisis and the geopolitical tensions, are shifting the narrative from one dominated by protracted low yields and low inflation to an economic juncture driven by high inflation and uncertain economic growth.

At the same time, EIOPA will continue to contribute to the recovery of the EU economy following the pandemic, supporting Member States in

building more resilient insurance and pensions sectors and further strengthening a common supervisory culture.

These times of transformation with uncertainties arising from an ever-changing macroeconomic environment, present potential increase in vulnerabilities of the insurance and pension sectors. Subsequently this calls for continued and forward-looking identification of risks in the context of a proactive and engaged supervisory community.

EIOPA will strive to provide supervisors with a reliable assessment of market vulnerabilities focusing on enhancing the methodological framework particularly for top-down and more streamlined vulnerability assessments while increasing capacity for emerging threats such as cyber and climate change.

Digitalisation, with its opportunities and risks, will require our attention to support the market and supervisory community through the digital transformation. As we see the digitalisation continue to accelerate, impacting business models, products and services as well as distribution channels, it is key to recognise threats and have measures in place that can keep the financial system safe and citizens included.

In addition to this, the digital transformation is also accelerating the interconnectedness of financial services, so that regulation is now becoming more horizontal.

EIOPA will strive to ensure that the insurance and pensions sectors are well represented in new cross-sectoral and horizontal regulation. Data is at the heart of the insurance and pension industry, and at the backbone of digital transformation and effective financial supervision.

To this end, EIOPA aims to enhance data availability and data standardisation, thus contributing to the development of a sound European Data Eco-System.

The insurance and pensions sectors have a unique opportunity and responsibility to address sustainabilityrelated challenges and thus facilitate the transition to a more sustainable and resilient economy, given their key role as society's risk managers and important long-term investors.

Addressing protection gaps remains a priority among EIOPA's activities on sustainable finance. EIOPA will step up its work on identifying protection gaps with the aim to promote coverage of risks and increasing their insurability, also through possible shared resilience solutions.

EIOPA will strive to further increase consumer risk awareness and understanding of riskbased prevention measures to climate change as well as complement the insurance and pensions sectors efforts for climate change mitigation and adaption by promoting open source data and modelling of climate change risks.

The transition to a more environmentally and socially sustainable economy will require assessing the possible impacts at macro-prudential level, as well as potential consumer detriment arising from greenwashing.

To achieve an even higher, more effective and further harmonised convergent level of supervision across the European Union, EIOPA will continue to strengthen supervisory convergence by ensuring consistent reviews and proportionate application of supervisory convergence tools, which shall remain fit-for-purpose.

At the same time, EIOPA will continue the monitoring of the implementation of supervisory convergence tools and follow-up measures at the national level.

The foundation for our supervision is good regulation. Solvency II, and particularly buffers, proved effective in protecting the insurance sector from market turmoil in the past economic crisis.

We need to make sure that Solvency II stays robust and fit for purpose taking into account that the European macroeconomic environment will remain challenging.

Additionally, EIOPA will step up its monitoring activities in order to ensure products are designed in the best interest of consumers, and can deliver value for money.

EIOPA aims to ensure that the products offered to policyholders offer value for money, that people's needs are put first before profit and that they are sold the products that are right for their individual situation.

Towards this end, EIOPA will strive to make sure that consumers have access to the right information and the right advice so they can make better informed decisions.

This includes efforts towards having disclosure documents that are truly consumer-focused and adapted for the digital age. In 2023 EIOPA will Chair the EU Agencies Network (EUAN) providing a forum for coordination, information exchange and agreement on common positions

on issues of shared interest thus helping shape informed policies and laws at the EU and national level.

Furthermore, EIOPA will plan and manage resources in an agile manner that allows accelerated decision-making and allocation of resources towards key priorities.

Looking forward, EIOPA will continue to develop as a responsible and attractive organisation, promoting diversity and inclusion. Good governance, cost-effective processes and strong partnerships will make the Authority well equipped to contribute to a future in which the insurance and pension sectors fulfil an essential role in underpinning a strong and sustainable recovery in Europe, for the benefit of citizens, business, and the economy.

To read more:
https://www.eiopa.europa.eu/sites/default/files/publications/administrative/eiopa-revised-spd-2023-2025.pdf

Number 7

Federal Reserve Board announces that six of the largest banks will participate in a pilot climate scenario analysis exercise

The Federal Reserve Board has announced that six of the nation's largest banks will participate in a pilot climate scenario analysis exercise designed to enhance the ability of supervisors and firms to measure and manage climate-related financial risks.

Scenario analysis—in which the resilience of financial institutions is assessed under different hypothetical climate scenarios—is an emerging tool to assess climate-related financial risks, and there will be no capital or supervisory implications from the pilot.

The pilot exercise will be launched in early 2023 and is expected to conclude around the end of the year.

At the beginning of the exercise, the Board will publish details of the climate, economic, and financial variables that make up the climate scenario narratives.

Over the course of the pilot, participating firms will analyze the impact of the scenarios on specific portfolios and business strategies.

The Board will then review firm analysis and engage with those firms to build capacity to manage climate-related financial risks.

The Board anticipates publishing insights gained from the pilot at an aggregate level, reflecting what has been learned about climate risk management practices and how insights from scenario analysis will help identify potential risks and promote risk management practices.
No firm-specific information will be released.

Climate scenario analysis is distinct and separate from bank stress tests. The Board's stress tests are designed to assess whether large banks have enough capital to continue lending to households and businesses during a severe recession.

The climate scenario analysis exercise, on the other hand, is exploratory in nature and does not have capital consequences.

By considering a range of possible future climate pathways and associated economic and financial developments, scenario analysis can assist firms and supervisors in understanding how climate-related financial risks may manifest and differ from historical experience.

The banks in the pilot exercise are:

- Bank of America,
- Citigroup,
- Goldman Sachs,
- JPMorgan Chase,
- Morgan Stanley,
- Wells Fargo.

In coming months, the Board will provide additional details on how the exercise will be conducted and the scenarios that will be used in the pilot.

Number 8

Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization

From November 2021 through January 2022, the Cybersecurity and Infrastructure Security Agency (CISA) responded to advanced persistent threat (APT) activity on a Defense Industrial Base (DIB) Sector organization's enterprise network.

During incident response activities, CISA uncovered that likely multiple APT groups compromised the organization's network, and some APT actors had long-term access to the environment.

APT actors used an open-source toolkit called Impacket to gain their foothold within the environment and further compromise the network, and also used a custom data exfiltration tool, CovalentStealer, to steal the victim's sensitive data.

This joint Cybersecurity Advisory (CSA) provides APT actors tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) identified during the incident response activities by CISA and a third-party incident response organization.

The CSA includes detection and mitigation actions to help organizations detect and prevent related APT activity.

CISA, the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) recommend DIB sector and other critical infrastructure organizations implement the mitigations in this CSA to ensure they are managing and reducing the impact of cyber threats to their networks.

Actions to Help Protect Against APT Cyber Activity.

- Enforce multifactor authentication (MFA) on all user accounts.
- Implement network segmentation to separate network segments based on role and functionality.
- Update software, including operating systems, applications, and firmware, on network assets.
- Audit account usage.

DETECTION

Given the actors' demonstrated capability to maintain persistent, long-term access in compromised enterprise environments, CISA, FBI, and NSA encourage organizations to:

1. Monitor logs for connections from unusual VPSs and VPNs. Examine connection logs for access from unexpected ranges, particularly from machines hosted by SurfShark and M247.

2. Monitor for suspicious account use (e.g., inappropriate or unauthorized use of administrator accounts, service accounts, or third-party accounts).

To read more:
https://www.cisa.gov/uscert/sites/default/files/publications/aa22-277a-impacket-and-exfiltration-tool-used-to-steal-sensitive-information-from-defense-industrial-base-organization.pdf

Number 9

BINDING OPERATIONAL DIRECTIVE 23-01

A web-friendly version of the *Cybersecurity and Infrastructure Security Agency's Binding Operational Directive 23-01 - Improving Asset Visibility and Vulnerability Detection on Federal Networks*.

A binding operational directive is a compulsory direction to federal, executive branch, departments and agencies for purposes of safeguarding federal information and information systems.

Section 3553(b)(2) of title 44, U.S. Code, authorizes the Secretary of the Department of Homeland Security (DHS) to develop and oversee the implementation of binding operational directives. Federal agencies are required to comply with these directives.

These directives do not apply to statutorily defined "national security systems" or to certain systems operated by the Department of Defense or the Intelligence Community.

This directive refers to the systems to which it applies as "Federal Civilian Executive Branch" systems, and to agencies operating those systems as "Federal Civilian Executive Branch" agencies.

Background

Continuous and comprehensive asset visibility is a basic pre-condition for any organization to effectively manage cybersecurity risk.

Accurate and up-to-date accounting of assets residing on federal networks is also critical for CISA to effectively manage cybersecurity for the Federal Civilian Executive Branch (FCEB) enterprise.

The purpose of this Binding Operational Directive is to make measurable progress toward enhancing visibility into agency assets and associated vulnerabilities.

While the requirements in this Directive are not sufficient for comprehensive, modern cyber defense operations, they are an important step to address current visibility challenges at the component, agency, and FCEB enterprise level.

The requirements of this Directive focus on two core activities essential to improving operational visibility for a successful cybersecurity program: asset discovery and vulnerability enumeration.

- **Asset discovery** is a building block of operational visibility, and it is defined as an activity through which an organization identifies what network addressable IP-assets reside on their networks and identifies the associated IP addresses (hosts).

  Asset discovery is non-intrusive and usually does not require special logical access privileges.

- **Vulnerability enumeration** identifies and reports suspected vulnerabilities on those assets. It detects host attributes (e.g., operating systems, applications, open ports, etc.), and attempts to identify outdated software versions, missing updates, and misconfigurations.

  It validates compliance with or deviations from security policies by identifying host attributes and matching them with information on known vulnerabilities.

  Understanding an asset's vulnerability posture is dependent on having appropriate privileges, which can be achieved through credentialed network-based scans or a client installed on the host endpoint.

Discovery of assets and vulnerabilities can be achieved through a variety of means, including active scanning, passive flow monitoring, querying logs, or in the case of software defined infrastructure, API query.

Many agencies' existing Continuous Diagnostics and Mitigation (CDM) implementations leverage such means to make progress toward intended levels of visibility.

Asset visibility is not an end in itself, but is necessary for updates, configuration management, and other security and lifecycle management activities that significantly reduce cybersecurity risk, along with exigent activities like vulnerability remediation.

The goal of this Directive is for agencies to comprehensively achieve the following outcomes without prescribing how to do so:

- Maintain an up-to-date inventory of networked assets as defined in the scope of this directive;

- Identify software vulnerabilities, using privileged or client-based means where technically feasible;

- Track how often the agency enumerates its assets, what coverage of its assets it achieves, and how current its vulnerability signatures are; and

- Provide asset and vulnerability information to CISA's CDM Federal Dashboard.

Agencies may request CISA's assistance in conducting an engineering survey to baseline current asset management capabilities. CISA will work with requesting agencies to provide technical and program assistance to resolve gaps, optimize scanning, and support achieving the required actions in this Directive.

To read more: https://www.cisa.gov/binding-operational-directive-23-01

https://www.cisa.gov/implementation-guidance-binding-operational-directive-23-01

BINDING OPERATIONAL DIRECTIVE 23-01 Questions and Answers

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Frequently Asked Questions

Q: What is the scope of this directive? Which devices specifically need to be scanned?

A: This directive applies to all IP-addressable networked assets that can be reached over IPv4 and IPv6 protocols.

An IP-addressable networked asset is defined as any reportable (i.e., non-ephemeral) information technology or operational technology asset

that is assigned an IPv4 or IPv6 address and accessible over IPv4 or IPv6 networks, regardless of the environment in which it operates.

The scope includes, but is not limited to, servers and workstations, virtual machines, routers and switches, firewalls, network appliances, and network printers — whether in on-premises, roaming, or cloud-operated deployment models.

The scope excludes ephemeral assets such as containers and third-party managed software as a service (SaaS) solutions.

Q: How does the pre-existing requirement to perform endpoint detection and response (EDR) differ from the requirements of this BOD? To what extent does EDR address asset visibility needs?

A: Asset visibility is a prerequisite for determining where to deploy EDR. While most EDR tools do not provide vulnerability information, the directive gives agencies the flexibility to use any tool that provides credential or client-level vulnerability information.

If an agency deploys EDR tools that can provide vulnerability information, those tools can be used in place of a client-based scanner.

Q: This BOD uses the term "networked assets." Does that imply cloud is out of scope?

A: Any non-ephemeral asset with an IP address is in scope, including applicable cloud assets. Many cloud use cases are unique. Many agencies have SaaS instances where agencies are unable to run their own scans.

In the case of traditional data center collocations, infrastructure as a service (IaaS), and in some cases platform as a service (PaaS), all assets with an IP address are in scope.

The scope excludes ephemeral assets such as containers and third-party managed SaaS solutions.

Q: Why does the directive say "initiate scans" instead of "execute" or "complete scans"?

A: Sometimes, especially in large enterprises, vulnerability scans may not be complete within the 14-day timeframe required in the BOD.

To overcome this issue, BOD 23-01 requires agencies to initiate a new scan every 14 days regardless of whether the previous scan has completed.

Agencies are also required to feed available results for the previous scan three days after the new scan is initiated, even when the previous scan is not fully complete.

Q: What is the difference between "asset management" and "asset discovery"?

A: Asset management and asset discovery are two distinct activities that frequently go hand in hand.

Asset management is the active monitoring and administration of endpoints using a centralized solution, such as unified endpoint management (UEM), mobile device management (MDM), or enterprise mobility management (EMM).

Inventories from asset management solutions may be used to feed the information about agency assets into the results of a comprehensive asset discovery effort.

Asset discovery is the process of checking an IPv4 or IPv6 network for active and inactive hosts (e.g., networked assets) by using a variety of methods. The most common discovery methods include actively trying to communicate with all IP addresses in a range using a scan tool such as **"nmap"** (which is only feasible on smaller IPv4 based networks), or by passively monitoring traffic on the wire to detect activity from any new assets.

Asset discovery helps organizations find unmanaged assets that are present on the network to ensure they are brought under appropriate management.

It also helps organizations identify networked devices, such as Internet of Things (IoT), that cannot be centrally managed. It is possible for an asset to fall off the management tool due to inactivity or other reasons, requiring it to be rediscovered.

Q: Why does the directive reference the software bill of materials (SBOM) in the Background section but not in subsequent sections?

A: SBOM is mentioned in the introduction to convey the Administration's vision and describe our desired state in the long term.

The directive focuses on very specific first steps that can be achieved within the next 6-12 months and are prerequisites for broader adoption of SBOM.

Without comprehensive asset management, agencies will be unable to effectively use SBOMs to manage risk posed by asset components or libraries.

Q: We offer public wireless access in conference rooms and lobbies. Are guest networks in scope?

A: Guest hosts are not in scope, provided the guest networks are physically segmented from agency networks.

Q: Are bring-your-own-device (BYOD) assets in scope?

A: Most federal agencies do not allow BYOD on enterprise networks. If they do, then BYOD devices are in scope.

This does not apply to personally owned equipment that connects to federal networks via web interface (e.g., website visitors or remote users connecting via SSL remote access solutions).

Q: Are air-gapped networks in scope? It may not be possible to transfer a signature to air-gapped networks within 24 hours.

A: Many logically isolated networks and systems are incorrectly considered air-gapped. Any device, system, or network that is directly connected to the operating environment, or is connected to another system that is connected to the operating environment, is not considered air-gapped and is in scope for BOD 23-01. Only systems that are truly physically air-gapped are out of scope.

Q: Does the BOD include requirements for scanning software and configuration enumerations?

A: No, the BOD requirements address only basic (IP) asset discovery and vulnerability enumeration.

The current BOD does not address hardware management, software management, or configuration management and associated controls.

Note that some vulnerabilities due to misconfigurations and basic configurations may be captured by standard vulnerability scanners.

Q: Which cloud assets are in scope?

A: Agencies are responsible for the discovery and enumeration of networked assets under agency control, such as assets in authority-to-operate (ATO) inventories.

Each cloud instance is unique, but in general, third-party hosting solutions where agencies still control physical or virtual hosts, such as infrastructure as a service, are within the scope of this directive.

Q: Are communications devices, such as IP telephony, VOIP phones, cameras, and unified communications peripherals in scope?

A: Yes, these devices are in scope. Adversaries have specifically targeted these devices as they are typically more difficult to harden.

Glossary

Vulnerability enumeration performance data – Otherwise referred to as scanning logs, vulnerability enumeration performance data describes datapoints or measurements that provide visibility on the level of performance relative to the requirements in this directive, using automation and machine-level data (e.g., logs/events indicating successful credentialed enumeration completion, date/timestamps surrounding enumeration activities, and signature/plug-in update date/timestamps). Data requirements to satisfy this objective will be published in a common data schema and made available to every Federal agency.

Vulnerability enumeration – A technique to list host attributes (e.g., operating systems, applications, and open ports) and associated vulnerabilities. Vulnerability enumeration typically requires privileged access to gain full visibility at the application and configuration levels.

Privileged credentials – A local or network account or a process with sufficient access to enumerate system configurations and software components across an entire asset. Administrators must apply the principle of least privilege and/or separation of duties on the accounts used for vulnerability enumeration. Poisoning and machine-in-the-middle type attacks commonly target accounts with elevated privileges, including those used for vulnerability enumeration.

Roaming devices – Devices that leave an agency's on-premises networks, connect to other private networks, and directly access the public internet.

Nomadic devices – Devices that permanently reside outside of agency networks.

To read more: https://www.cisa.gov/binding-operational-directive-23-01

https://www.cisa.gov/implementation-guidance-binding-operational-directive-23-01

Number 10

Scientists chip away at a metallic mystery, one atom at a time

It's no secret that radiation weakens metal. Uncovering how is complicated work.

Sandia National Laboratories

Gray and white flecks skitter erratically on a computer screen. A towering microscope looms over a landscape of electronic and optical equipment.

Inside the microscope, high-energy, accelerated ions bombard a flake of platinum thinner than a hair on a mosquito's back.

Meanwhile, a team of scientists studies the seemingly chaotic display, searching for clues to explain how and why materials degrade in extreme environments.

Based at Sandia, these scientists believe the key to preventing large-scale, catastrophic failures in bridges, airplanes and power plants is to look — very closely — at damage as it first appears at the atomic and nanoscale levels.

"As humans, we see the physical space around us, and we imagine that everything is permanent," Sandia materials scientist Brad Boyce said. "We see the table, the chair, the lamp, the lights, and we imagine it's always going to be there, and it's stable. But we also have this human experience that things around us can unexpectedly break. And that's the evidence that these things aren't really stable at all. The reality is many of the materials around us are unstable."

But the ground truth about how failure begins atom by atom is largely a mystery, especially in complex, extreme environments like space, a fusion reactor or a nuclear power plant. The answer is obscured by complicated, interconnected processes that require a mix of specialized expertise to sort out.

The team recently published in the academic journal Science Advances research results on the destabilizing effects of radiation. While the findings describe how metals degrade from a fundamental perspective, the results could potentially help engineers predict a material's response to different kinds of damage and improve the reliability of materials in intense radiation environments.

For instance, by the time a nuclear power plant reaches retirement age, pipes, cables and containment systems inside the reactor can be dangerously brittle and weak. Decades of exposure to heat, stress, vibration and a constant barrage of radiation break down materials faster than normal. Formerly strong structures become unreliable and unsafe, fit only for decontamination and disposal.

“If we can understand these mechanisms and make sure that future materials are, basically, adapted to minimize these degradation pathways, then perhaps we can get more life out of the materials that we rely on, or at least better anticipate when they’re going to fail so we can respond accordingly,” Boyce said.

The research was performed, in part, at the Center for Integrated Nanotechnologies, an Office of Science user facility operated for DOE by Sandia and Los Alamos national laboratories. It was funded by the DOE’s Basic Energy Sciences program.

Atomic-scale research could protect metals from damage

Metals and ceramics are made up of microscopic crystals, also called grains. The smaller the crystals, the stronger materials tend to be. Scientists have already shown it is possible to strengthen a metal by engineering incredibly small, nanosized crystals.

“You can take pure copper, and by processing it so that the grains are nanosized, it can become as strong as some steels,” Boyce said.

But radiation smashes and permanently alters the crystal structure of grains, weakening metals. A single radiation particle strikes a crystal of metal like a cue ball breaks a neatly racked set of billiard balls, said Rémi Dingreville, a computer simulation and theory expert on the team. Radiation might only strike one atom head on, but that atom then pops out of place and collides with others in a chaotic domino effect.

Unlike a cue ball, Dingreville said, radiation particles pack so much heat and energy that they can momentarily melt the spot where they hit, which also weakens the metal. And in heavy-radiation environments, structures live in a never-ending hailstorm of these particles.

The Sandia team wants to slow — or even stop — the atomic-scale changes to metals that radiation causes. To do that, the researchers work like forensic investigators replicating crime scenes to understand real ones. Their Science Advances paper details an experiment in which they used

their high-powered, highly customized electron microscope to view the damage in the platinum metal grains.

Team member Khalid Hattar has been modifying and upgrading this microscope for over a decade, currently housed in Sandia's Ion Beam Laboratory. This one-of-a-kind instrument can expose materials to all sorts of elements — including heat, cryogenic cold, mechanical strain, and a range of controlled radiation, chemical and electrical environments. It allows scientists to watch degradation occur microscopically, in real time. The Sandia team combined these dynamic observations with even higher magnification microscopy allowing them to see the atomic structure of the boundaries between the grains and determine how the irradiation altered it.

But such forensics work is fraught with challenges.

"I mean, these are extremely hard problems," said Doug Medlin, another member of the Sandia team. Boyce asked for Medlin's help on the project because of his deep expertise in analyzing grain boundaries. Medlin has been studying similar problems since the 1990s.

"We're starting from a specimen that's maybe three millimeters in diameter when they stick it into the electron microscope," Medlin said. "And then we're zooming down to dimensions that are just a few atoms wide. And so, there's just that practical aspect of: How do you go and find things before and after the experiment? And then, how do you make sense of those atomistic arrangements in a meaningful way?"

By combining atomic-scale images with nanoscale video collected during the experiment, the team discovered that irradiating the platinum causes the boundaries between grains to move.

Computer simulations help explain cause and effect

After the experiment, their next challenge was to translate what they saw in images and video into mathematical models. This is difficult when some atoms might be dislocated because of physical collisions, while others might be moving around because of localized heating. To separate the effects, experimentalists turn to theoreticians like Dingreville.

"Simulating radiation damage at the atomic scale is very (computationally) expensive," Dingreville said. Because there are so many moving atoms, it takes a lot of time and processing power on high-performance computers to model the damage.

Sandia has some of the best modeling capabilities and expertise in the world, he said. Researchers commonly measure the amount of damage radiation causes to a material in units called displacements per atom, or dpa for short. Typical computer models can simulate up to around 0.5 dpa worth of damage. Sandia models can simulate up to 10 times that, around 5 dpa.

In fact, the combination of in-house expertise in atomic microscopy, the ability to reproduce extreme radiation environments and this specialized niche of computer modeling makes Sandia one of few places in the world where this research can take place, Dingreville said.

But even Sandia's high-end software can only simulate a few seconds' worth of radiation damage. An even better understanding of the fundamental processes will require hardware and software that can simulate longer spans of time. Humans have been making and breaking metals for centuries, so the remaining knowledge gaps are complex, Boyce said, requiring expert teams that spend years honing their skills and refining their theories. Medlin said the long-term nature of the research is one thing that has attracted him to this field of work for nearly 30 years.

"I guess that's what drives me," he said. "It's this itch to figure it out, and it takes a long time to figure it out."

Note: Sandia National Laboratories is a multimission laboratory operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration. Sandia Labs has major research and development responsibilities in nuclear deterrence, global security, defense, energy technologies and economic competitiveness, with main facilities in Albuquerque, New Mexico, and Livermore, California.

To read more: https://newsreleases.sandia.gov/material_degradation/

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)

You can explore what we offer to our members:

1. *Membership* – Become a standard, premium or lifetime member.

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

2. *Weekly Updates* - Visit the *Reading Room* of the association at:
https://www.risk-compliance-association.com/Reading_Room.htm

3. *Training and Certification* – Become:

- a Certified Risk and Compliance Management Professional (CRCMP),

- a Certified Information Systems Risk and Compliance Professional (CISRCP),

- a Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P,

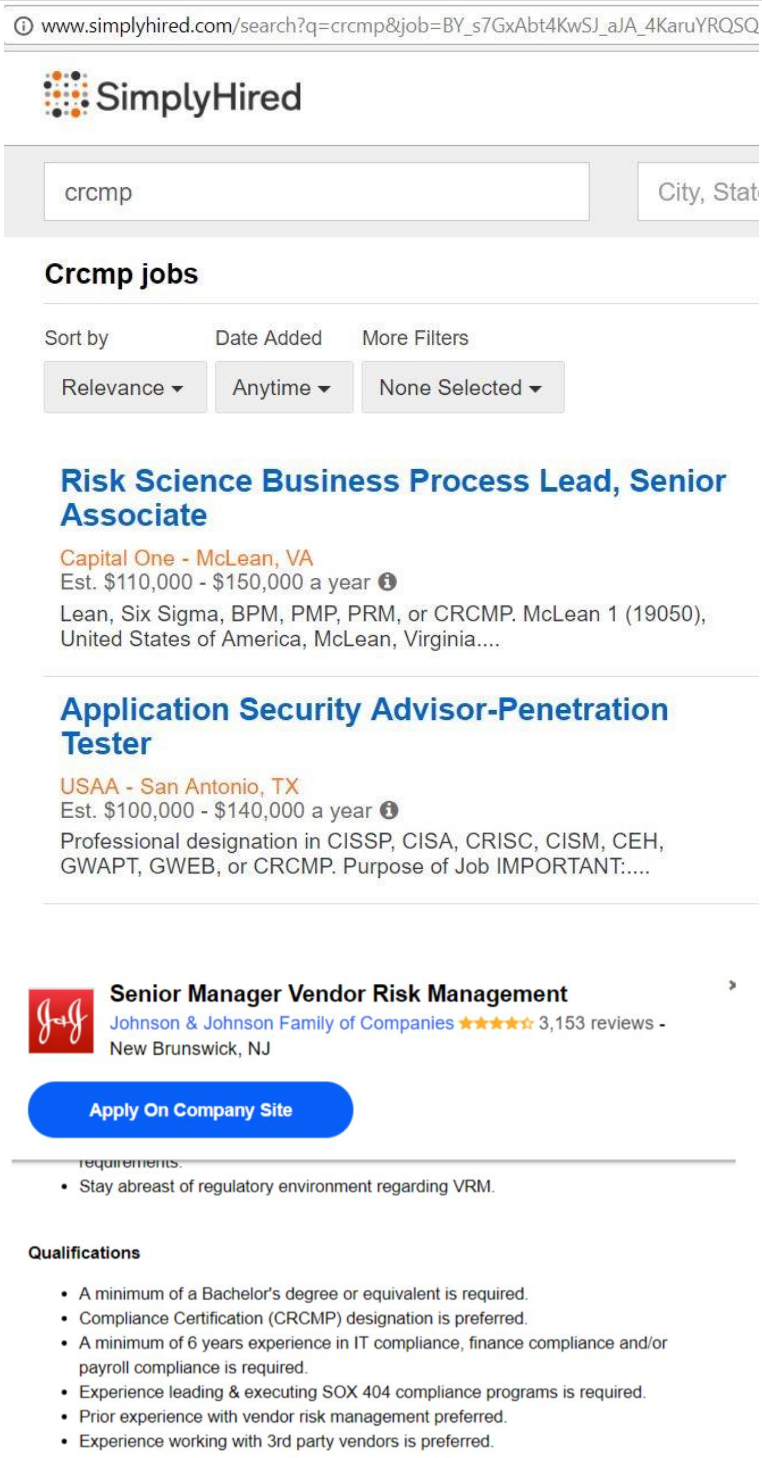
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- a Travel Security Trained Professional (TSecTPro).

The CRCMP has become one of the most recognized certificates in risk management and compliance. There are CRCMPs in 32 countries.

Companies and organizations around the world consider the CRCMP a preferred certificate:

Senior Information Security Risk Analyst
Public Company Accounting Oversight Board - ★★★★☆ 10 reviews - Washington, DC
Professional designation in CISSP, CISA, CRISC, or CRCMP preferred. The PCAOB is a nonprofit corporation established by Congress to oversee the audits of public...



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

For the 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

For the 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

For the 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

For the 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

For the 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

Certified Cyber (Governance Risk and Compliance) Professionals - CC(GRC)Ps, have a 50% discount for the Travel Security Trained Professional (TSecTPro) program ($148 instead of $297).

You have a $100 discount after you purchase one of our programs. The discount applies to each additional program. For example, you can purchase the CRCMP program for $297, and then purchase the CISRCP program for $197 (instead of $297), the CC(GRC)P program for $197 (instead of $297), the CRCMP(Re)I program for $197 (instead of $297), and the TSecTPro program for $197 (instead of $297).

For *instructor-led* training, you may contact us. We can tailor all programs to meet specific requirements.