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, May 1, 2023

Top 10 risk and compliance related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next

Dear members and friends,

Lucius Annaeus Seneca has said: “It is not because things are difficult that we do not dare, it is because we do not dare that they are difficult.”

Dear Lucius, even if we dare, things are becoming very difficult for the healthcare industry, and the regulatory landscape becomes way more complex. Healthcare compliance officers may need some medical assistance in the near future, but at least they work in the right place for that.

It is very difficult to achieve a balance between the need for patient access to affordable medicinal products and the need to stimulate innovation.

The European Commission has just introduced *two* legislative proposals, a directive and a regulation for medicinal products. Why should we choose between a directive and a regulation, when we can have both?

The *proposal for a Regulation* "laying down Union procedures for the authorisation and supervision of medicinal products for human use and establishing rules governing the European Medicines Agency", is *182 pages long*. It covers the authorisation, supervision and pharmacovigilance of medicinal products for human use at Union level, and establishes rules and procedures at Union and at Member State level relating to the *security of supply* of medicinal products.

The Regulation will not affect the powers of Member States' authorities as regards *setting the prices* of medicinal products, or their *inclusion in the scope* of the national health system or social security schemes on the basis of health, economic and social conditions.

The *proposal for a Directive* "on the Union code relating to medicinal products for human use" is *184 pages long*. It covers rules for the *placing on the market, manufacturing, import, export, supply, distribution,* pharmacovigilance, control and use of medicinal products for human use.

These two legal acts are on top of the *proposed European Health Data Space (EHDS),* a key pillar of the *European Health Union* that builds further on the General Data Protection Regulation (GDPR) and the NIS 2 Directive. Yes, it is becoming very complex and difficult to understand.

The European Health Union covers how EU countries prepare and respond to health crises, have available, affordable, innovative and adequate medical supplies, and work together to improve prevention, treatment and aftercare for diseases.

The proposed EHDS regulation applies to:

(a) manufacturers and suppliers of electronic health record (HER) systems and wellness applications placed on the market and put into service in the Union and the users of such products;

(b) controllers and processors established in the Union processing electronic health data of Union citizens and third-country nationals legally residing in the territories of Member States;

(c) controllers and processors established in a third country that has been connected to or are interoperable with MyHealth@EU;

There are interesting *security related* definitions too. In the proposed EHDS regulation we read:

'Serious incident' means any malfunction or deterioration in the

characteristics or performance of an EHR system made available on the market that directly or indirectly leads, might have led or might lead to any of the following:

(i) the death of a natural person or serious damage to a natural person's health;

(ii) a serious disruption of the management and operation of critical infrastructure in the health sector;

Marcus Tullius Cicero has said that "It is the peculiar quality of a fool to perceive the faults of others and to forget his own". There are no fools in the European Commission, and they definitely do not want to forger their own mistakes in the past, so they try to make no mistakes now. How can you forget something in a legal act if you call "serious incident" something that might have led or might lead to problems?

The list of the 'serious incidents' is probably very long. If we combine it with the "all-hazards approach" in the NIS 2 Directive, risk and compliance officers in the future will have to spend way more time learning and understanding the legal aspects, in a very complex environment.

Read more at number 6 and 7 below. Welcome to the Top 10 list.

Best regards,

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

Number 1 (Page 6)

EIOPA and ECB call for increased uptake of climate catastrophe insurance

Number 2 (Page 10)

2022 Annual Report

Number 3 (Page 14)

Recommendations to Achieve Greater Convergence in Cyber Incident Reporting, Final Report

Number 4 (Page 19)

Supercharging security with generative AI

Sunil Potti, VP/GM, Google Cloud Security

Number 5 (Page 21)

Introducing Microsoft Security Copilot: Empowering defenders at the speed of AI

Number 6 (Page 23)

Proposal for a Regulation,

laying down Union procedures for the authorisation and supervision of medicinal products for human use and establishing rules governing the European Medicines Agency.

Number 7 (Page 25)

Proposal for a Directive,

on the Union code relating to medicinal products for human use,

EUROPEAN COMMISSION

Number 8 (Page 27)

Active Cyber Defence (ACD) program - The Sixth Year

Key findings from the 6th year of the ACD program

National Cyber Security Centre

Number 9 (Page 30)

ESAs call for vigilance in the face of mounting financial risks

EBA EUROPEAN BANKING AUTHORITY

eiopa European Insurance and Occupational Pensions Authority

ESMA European Securities and Markets Authority

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Number 10 (Page 32)

Developing Agile, Reliable Sensing Systems with Microbes

DARPA's Tellus program seeks to advance remote environmental sense-and-respond platforms with enhanced breadth, resolution

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 1

EIOPA and ECB call for increased uptake of climate catastrophe insurance

The European Insurance and Occupational Pensions Authority (EIOPA) and the European Central Bank (ECB) published a joint discussion paper on how to better insure households and businesses in the European Union against climate-related natural catastrophes such as floods or wildfires.

The policy options set out in the paper are aimed at boosting the uptake and efficiency of climate catastrophe insurance while creating incentives to adapt to and reduce climate risks.

“We need to increase the uptake of climate catastrophe insurance to limit the growing impact of natural disasters on the economy and the financial system,” said ECB Vice-President Luis de Guindos. “However, to reduce losses in the first place, we must ensure that a smooth and speedy green transition is complemented by effective measures to adapt to climate change.”

EIOPA Chairperson Petra Hielkema added: “Insurance plays a major role in protecting businesses and people against climate-related catastrophe losses by swiftly providing the necessary funds for reconstruction. In order to efficiently protect our society, we need to address the concern of the increasing insurance protection gap by proposing and finding appropriate solutions.”

Currently, only about one-quarter of all climate-related catastrophe losses in the European Union are insured. In some countries, the figure is below 5%. This is partly because many people underestimate the costs of climate-related damage. Some also shy away from insurance, preferring to rely on government support.

As natural disasters become both more frequent and more severe, insurance costs are expected to rise. Some insurers may reduce risk coverage or stop providing certain types of catastrophe insurance altogether, which would widen the insurance gap further.

The lack of climate catastrophe insurance can affect the economy and financial stability. If losses are not covered by insurance, the speed at which households and firms can resume their activities is reduced, slowing economic recovery.

Lasting supply chain disruptions can also lead to spillovers from one firm to another and affect firms' ability to pay back loans, thereby increasing banks' exposures to credit risk. Additionally, the financial position of governments may be weakened if they need to provide relief to cover uninsured losses.

To foster insurance coverage, EIOPA and the ECB suggest that insurers should design their policies to encourage households and firms to reduce risk, for example by granting discounts for implementing effective mitigation or adaptation measures.

To support the overall supply of insurance, the use of catastrophe bonds could be increased to pass on part of the risk to capital market investors. In the same vein, governments could set up public-private partnerships and backstops to partly cover the costs that insurers may incur in the event of major disasters.

To protect themselves and ensure that public funds are used efficiently, governments should also provide strong incentives to reduce risks.

Finally, national-level insurance schemes could be complemented by an EU-wide public scheme that makes sure sufficient funds are made available to European countries for reconstruction following rare, large-scale climate-related catastrophes.

The joint discussion paper is part of the EIOPA's sustainable finance agenda and its work to improve the overall understanding of climate-related risk. The paper aims to foster debate on how to tackle the climate insurance protection gap.

EIOPA and the ECB will collect feedback on the policy options and also discuss them in a workshop with regulators, policymakers, insurers and academics on 22 May 2023.

Policy options to reduce the climate insurance protection gap

Discussion Paper

Executive summary 2

Introduction 5

1 The economic relevance of the climate insurance protection gap 9

1.1 Implications for the macroeconomy 9

1.2 Implications for the financial system 12

1.3 Fiscal implications 13

2 Potential policy measures to reduce the climate insurance protection gap – the ladder approach 16

2.1 Layer 1: Low to moderate loss layers: potential measures to enhance private insurance and impact underwriting 18

2.2 Layer 2: Higher loss layers: potential measures relating to reinsurance and catastrophe bonds 19

Box 1 A closer look at the cat bond market 21

2.3 Layer 3: National measures – the role of the public sector 24

2.4 Layer 4: EU-level measures 28

Box 2 Addressing moral hazard 33

3 Complementarity with wider EU policy initiatives 36

4 Conclusion 38

5 Appendix 39

6 References 41

Executive summary

Extreme weather and climate events can have significant macroeconomic implications. While the economic impact of such events in Europe has been manageable historically, it is expected to rise over time as catastrophes become more frequent and more severe due to global warming.

Catastrophe insurance is a key tool to mitigate macroeconomic losses following extreme climate-related events, as it provides prompt funding for reconstruction and should incentivise risk reduction and adaptation.

The overall societal cost of a disaster depends not only on the severity of the initial damage but also on how swiftly reconstruction can be completed. However, reconstruction can be prolonged and may even be incomplete in the absence of sufficient resources. Insurance payouts reduce uncertainty and support aggregate demand and investment for reconstruction, enabling economies to recover faster and limiting the period of lower economic output.

By contrast, without insurance, households and firms have to finance post-disaster recovery mainly with savings, credit and/or uncertain government relief, which is likely to be much less efficient.

Only about a quarter of climate-related catastrophe losses are currently insured in the EU. This insurance protection gap could widen in the medium to long term as a result of climate change, partly because repricing of insurance contracts in response to increasingly frequent and intense events may lead to such insurance becoming unaffordable.

This would further increase the burden on governments, both in terms of macroeconomic risks and in terms of fiscal spending to cover uninsured losses. This may raise government debt burdens of EU countries and increase economic divergence.

A widening insurance protection gap may also pose financial stability risks and reduce credit provision in countries with large banking sector exposures to catastrophe risk events.

This discussion paper sets out possible actions which should be considered to tackle this protection gap and mitigate catastrophe risks from climate change in the EU by means of insurance coverage and adaptation measures.

These efforts should be complementary to ambitious mitigation policies to tackle climate change and reduce associated catastrophe risks, and should not be seen as a substitute for such policies.

To read more:
https://www.eiopa.europa.eu/system/files/2023-04/ecb.policyoptions_EIOPA~c0adae58b7.en_.pdf

Number 2

2022 Annual Report

PCAOB
PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD

Goal One: Modernize Standards

Effective standards advance audit quality and are foundational to the PCAOB's execution of its mission to protect investors. Not only do our standards provide the requirements auditors must satisfy when conducting their audits, they also serve as the basis for our inspection and enforcement activities.

When the PCAOB was first getting off the ground in 2003, it adopted existing standards that had been set by the auditing profession on what was intended to be an interim basis.

Twenty years later, far too many of those interim standards remain unchanged. The world has changed since 2003. And our standards must adapt to keep up with developments in auditing and the capital markets.

So in 2022, the Board announced one of the most ambitious standard-setting agendas in PCAOB history, and our staff began work on more than 30 standards within 13 standard-setting and research projects.

Goal Two: Enhance Inspections

Inspecting registered public accounting firms is one of the most important tools the PCAOB uses to protect investors.

In fact, the Division of Registration and Inspections is our largest division, with over 460 dedicated professionals inspecting roughly 200 audit firms and 800 audit engagements in more than 30 jurisdictions around the world each year.

PCAOB inspections determine whether firms are complying with PCAOB standards meant to protect investors, and inspectors' work can also provide information that may lead to PCAOB investigations and enforcement actions, as well as standard setting.

The PCAOB's inspection reports provide valuable information to investors, audit committees, and others to help inform their decisions. And the inspection process is the PCAOB's principal means of evaluating the state of audit quality to best keep investors protected.

In 2022, the PCAOB also enhanced its inspections by adapting to emerging risks and issues around the world and providing new insights. Additionally, the PCAOB is now inspecting registered firms in Mainland China and Hong Kong for the first time in PCAOB history. (See page 10 for more on the PCAOB's work to gain complete access to inspect and investigate firms in Mainland China and Hong Kong.)

Goal Three: Strengthen Enforcement

The PCAOB's enforcement program protects investors by holding accountable those who put investors at risk by violating PCAOB rules and standards and other related laws and rules. Strong enforcement and meaningful sanctions also deter wrongdoing.

In 2022, the PCAOB approached enforcement with a renewed vigilance, increasing average penalties, pursuing enforcement actions involving certain types of violations for the first time, and taking steps to identify wrongdoing proactively by expanding the use of sweeps of firms to determine whether there may be a violation of PCAOB standards or rules.

Goal Four: Improve Organizational Effectiveness

The PCAOB's most valuable resource is people, including the more than 800 dedicated professionals on our staff who carry out our mission, as well as external stakeholders whose input makes us more effective.

In 2022, the PCAOB took significant steps to invest in our staff and to enhance our stakeholder engagement.

Strategic Goals

The PCAOB's 2022-2026 strategic plan sets out four strategic goals that guide the organization's efforts to achieve its mission of protecting investors.

Protecting Investors Through One of the Most Ambitious Standard-Setting Agendas in PCAOB History

The PCAOB made progress after updating its standard-setting and research agendas in 2022. More remains to be done. As of December 31, 2022, these were the PCAOB's active research and standard-setting projects. Track and learn more about these projects at **www.pcaobus.org/standards**. *(See page 14 for more on the PCAOB's advisory groups, which in 2022 provided perspective on our standard-setting and research agendas.)*

Short-Term Standard-Setting Projects

- Quality Control
- Confirmation
- Noncompliance with Laws and Regulations
- Attestation Standards Update
- Going Concern
- Interim Standards – AS 1000
- Amendments Related to Certain Aspects of Designing and Performing Audit Procedures that Involve Technology-Assisted Data Analysis

Mid-Term Standard-Setting Projects

- Substantive Analytical Procedures
- Fraud
- Interim Ethics and Independence Standards
- Interim Standards

Research Projects

- Data and Technology
- Firm and Engagement Performance Metrics

Erica Y. Williams
Chair

Duane M. DesParte
Board Member

Christina Ho
Board Member

Kara M. Stein
Board Member

Anthony C. Thompson
Board Member

The report:
https://assets.pcaobus.org/pcaob-dev/docs/default-source/about/administration/documents/annual_reports/2022-annual-report_final.pdf?sfvrsn=d73be283_2

Number 3

Recommendations to Achieve Greater Convergence in Cyber Incident Reporting, Final Report

FSB FINANCIAL STABILITY BOARD

Executive summary

Cyber incidents are rapidly growing in frequency and sophistication. At the same time, the cyber threat landscape is expanding amid digital transformation, increased dependencies on third party service providers and geopolitical tensions.

The interconnectedness of the global financial system makes it possible that a cyber incident at one financial institution (FI) (or an incident at one of its third-party service providers) could have spill-over effects across borders and sectors.

Recognising that timely and accurate information on cyber incidents is crucial for effective incident response and recovery and promoting financial stability, the G20 asked the FSB to deliver a report on achieving greater convergence in cyber incident reporting (CIR).

To meet this call, the FSB conducted work to promote greater convergence in CIR in three ways:

(i) setting out recommendations to address the issues identified as impediments to achieving greater harmonisation in incident reporting;

(ii) enhancing the Cyber Lexicon1 to include additional terms related to CIR as a 'common language' is necessary for increased convergence; and

(iii) identifying common types of information that are submitted by FIs to authorities for CIR purposes, which culminated in a concept for a common format for incident reporting exchange (FIRE) to collect incident information from FIs and use between themselves.

FIRE would be flexible to allow a range of adoption choices and include the most relevant data elements for financial authorities.

Drawing from the FSB's body of work on cyber, including engagement with external stakeholders, this report sets out recommendations that aim to promote convergence among CIR frameworks, while recognising that a one-size-fits-all approach is not feasible or preferable.

Financial authorities and FIs can choose to adopt these recommendations as appropriate and relevant, consistent with their legal and regulatory framework.

Table of Contents

Executive summary 1
1. Introduction 3
2. Practical issues and challenges to achieving greater convergence in CIR 3
2.1. Operational challenges 4
2.2. Setting reporting criteria 8
2.3. Culture of timely reporting 8
2.4. Early assessment challenges 10
2.5. Secure communications 10
2.6. Cross-border and cross-sectoral issues 11
3. Recommendations 11
3.1. Design of approach to CIR 11
3.2. Supervisory activities and collaboration betweenauthorities 18
3.3. Industry engagement 20
3.4. Capability development (individual and shared) 21
Annex A: 2022 Survey findings 24
Annex B: Recommendations mapped to identified issues and challenges 32
Annex C: Initial reporting trigger reference material 33

Recommendations:

1. **Establish and maintain objectives for CIR.** Financial authorities should have clearly defined objectives for incident reporting, and periodically assess and demonstrate how these objectives can be achieved in an efficient manner, both for FIs and authorities.

2. **Explore greater convergence of CIR frameworks.** Financial authorities should continue to explore ways to align their CIR regimes with other relevant authorities, on a cross-border and cross-sectoral basis, to minimise potential fragmentation and improve interoperability.

3. **Adopt common data requirements and reporting formats.** Financial authorities should individually or collectively identify common data requirements, and, where appropriate, develop or adopt standardised formats for the exchange of incident reporting information.

4. **Implement phased and incremental reporting requirements.** Financial authorities should implement incremental reporting

requirements in a phased manner, balancing the authority's need for timely reporting with the affected institution's primary objective of bringing the incident under control.

5. **Select appropriate incident reporting triggers.** Financial authorities should explore the benefits and implications of a range of reporting trigger options as part of the design of their CIR regime.

6. **Calibrate initial reporting windows.** Financial authorities should consider potential outcomes associated with window design or calibration used for initial reporting.

7. **Provide sufficient details to minimise interpretation risk.** Financial authorities should promote consistent understanding and minimise interpretation risk by providing an appropriate level of detail in setting reporting thresholds, using common terminologies and supplementing CIR guidance with examples.

8. **Promote timely reporting under materiality-based triggers.** Financial authorities that use materiality thresholds should consider finetuning threshold language, or explore other suitable approaches, to encourage prompt reporting by FIs for material incidents.

9. **Review the effectiveness of CIR and cyber incident response and recovery (CIRR) processes.** Financial authorities should explore ways to review the effectiveness of FIs' CIR and CIRR processes and procedures as part of their existing supervisory or regulatory engagement.

10. **Conduct ad-hoc data collection.** Financial authorities should explore ways to complement CIR frameworks with supervisory measures as needed and engage FIs on cyber incidents, both during and outside of live incidents.

11. **Address impediments to cross-border information sharing.** Financial authorities should explore methods for collaboratively addressing legal or confidentiality challenges relating to the exchange of CIR information on a cross-border basis.

12. **Foster mutual understanding of benefits of reporting.** Financial authorities should engage regularly with FIs to raise awareness of the value and importance of incident reporting, understand possible challenges faced by FIs and identify approaches to overcome them when warranted.

13. **Provide guidance on effective CIR communication.** Financial authorities should explore ways to develop, or foster development of, toolkits and guidelines to promote effective communication practices in cyber incident reports.

14. **Maintain response capabilities which support CIR.** FIs should continuously identify and address any gaps in their cyber incident response capabilities which directly support CIR, including incident detection, assessment and training on a continuous basis.

15. **Pool knowledge to identify related cyber events and cyber incidents.** Financial authorities and FIs should collaborate to identify and implement mechanisms to proactively share event, vulnerability and incident information amongst financial sector participants to combat situational uncertainty, and pool knowledge in collective defence of the financial sector.

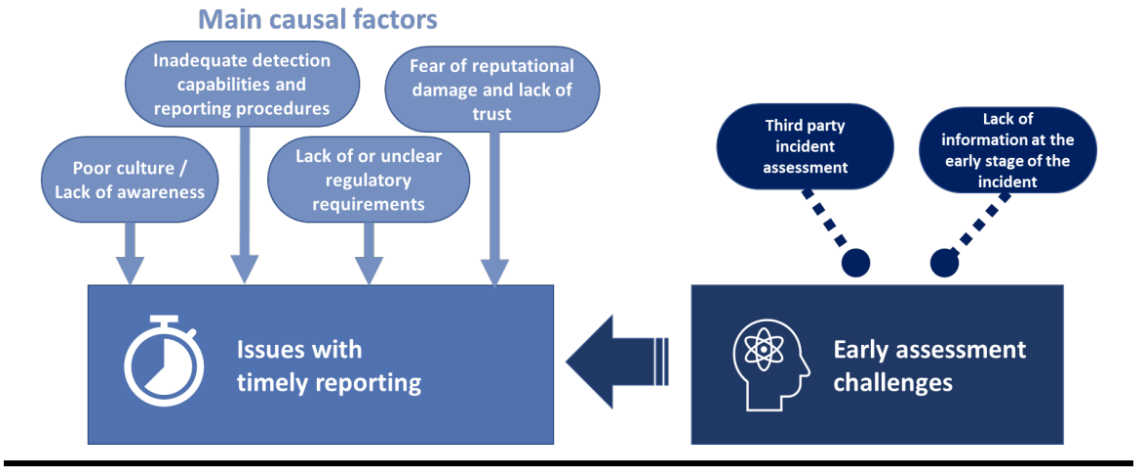
16. **Protect sensitive information.** Financial authorities should implement secure forms of incident information handling to ensure protection of sensitive information at all times.

FSB FINANCIAL STABILITY BOARD

Recommendations to Achieve Greater Convergence in Cyber Incident Reporting

Final Report

Possible causal factors to issues with timely reporting Figure 3



The report: https://www.fsb.org/wp-content/uploads/P130423-1.pdf

Number 4

Supercharging security with generative AI

Sunil Potti, VP/GM, Google Cloud Security

Google Cloud

At Google Cloud, we continue to invest in key technologies to progress towards our true north star on invisible security: making strong security pervasive and simple for everyone.

Our investments are based on insights from our world-class threat intelligence teams and experience helping customers respond to the most sophisticated cyberattacks.

Customers can tap into these capabilities to gain perspective and visibility on the most dangerous threat actors that no one else has.

Recent advances in artificial intelligence (AI), particularly large language models (LLMs), accelerate our ability to help the people who are responsible for keeping their organizations safe.

These new models not only give people a more natural and creative way to understand and manage security, they give people access to AI-powered expertise to go beyond what they could do alone.

At the RSA Conference 2023, we are excited to announce Google Cloud Security AI Workbench, an industry-first extensible platform powered by a specialized, security LLM, Sec-PaLM.

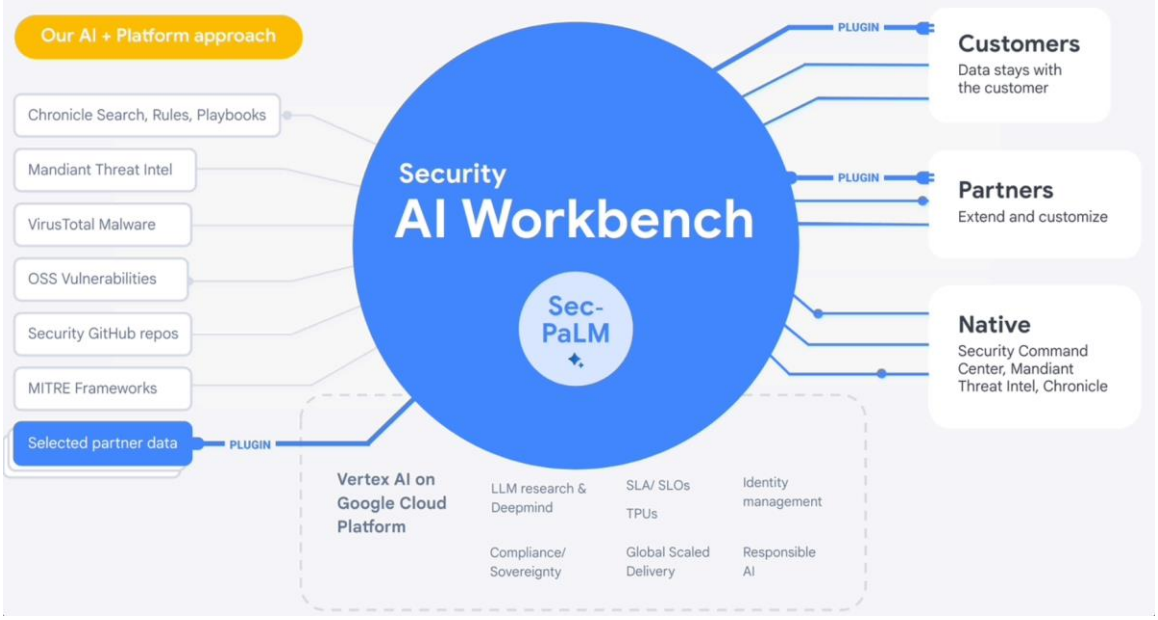
This new security model is fine-tuned for security use cases, incorporating our unsurpassed security intelligence such as Google's visibility into the threat landscape and Mandiant's frontline intelligence on vulnerabilities, malware, threat indicators, and behavioral threat actor profiles.

Google Cloud Security AI Workbench powers new offerings that can now uniquely address three top security challenges: threat overload, toilsome tools, and the talent gap.

It will also feature partner plug-in integrations to bring threat intelligence, workflow, and other critical security functionality to customers, with Accenture being the first partner to utilize Security AI Workbench.

The platform will also let customers make their private data available to the platform at inference time; ensuring we honor all our data privacy commitments to customers.

Because Security AI Workbench is built on Google Cloud's Vertex AI infrastructure, customers control their data with enterprise-grade capabilities such as data isolation, data protection, sovereignty, and compliance support.



To read more:
https://cloud.google.com/blog/products/identity-security/rsa-google-cloud-security-ai-workbench-generative-ai

Number 5

Introducing Microsoft Security Copilot: Empowering defenders at the speed of AI

Microsoft

Today the odds remain stacked against cybersecurity professionals. Too often, they fight an asymmetric battle against prolific, relentless and sophisticated attackers.

To protect their organizations, defenders must respond to threats that are often hidden among noise.

Compounding this challenge is a global shortage of skilled security professionals, leading to an estimated 3.4 million openings in the field.

The volume and velocity of attacks requires us to continually create new technologies that can tip the scales in favor of defenders.

Security professionals are scarce, and we must empower them to disrupt attackers' traditional advantages and drive innovation for their organizations.

In the last few months, the world has witnessed a wave of innovation as organizations apply advanced AI to new technologies and use cases.

We are ready for a paradigm shift and taking a massive leap forward by combining Microsoft's leading security technologies with the latest advancements in AI.

Security Copilot — end-to-end defense at machine speed and scale

Microsoft Security Copilot is the first security product to enable defenders to move at the speed and scale of AI. Security Copilot combines this advanced large language model (LLM) with a security-specific model from Microsoft.

This security-specific model in turn incorporates a growing set of security-specific skills and is informed by Microsoft's unique global threat intelligence and more than 65 trillion daily signals.

Security Copilot also delivers an enterprise-grade security and privacy-compliant experience as it runs on Azure's hyperscale infrastructure.

When Security Copilot receives a prompt from a security professional, it uses the full power of the security-specific model to deploy skills and queries that maximize the value of the latest large language model capabilities. And this is unique to a security use-case.

Our cyber-trained model adds a learning system to create and tune new skills. Security Copilot then can help catch what other approaches might miss and augment an analyst's work. In a typical incident, this boost translates into gains in the quality of detection, speed of response and ability to strengthen security posture. Security Copilot doesn't always get everything right. AI-generated content can contain mistakes.

But Security Copilot is a closed-loop learning system, which means it's continually learning from users and giving them the opportunity to give explicit feedback with the feedback feature that is built directly into the tool.

As we continue to learn from these interactions, we are adjusting its responses to create more coherent, relevant and useful answers.

Security Copilot also integrates with the end-to-end Microsoft Security products, and over time it will expand to a growing ecosystem of third-party products. So, in short, Security Copilot is not only a large language model, but rather a system that learns, to enable organizations to truly defend at machine speed.

We absolutely believe that security is a team sport, and security should be built with privacy at the core. We've built Security Copilot with security teams in mind— your data is always your data and stays within your control.

It is not used to train the foundation AI models, and in fact, it is protected by the most comprehensive enterprise compliance and security controls. While remaining private, each user interaction can be easily shared with other team members to accelerate incident response, collaborate more effectively on complex problems and develop collective skills.

To read more: https://news.microsoft.com/ai-security-2023/

Number 6

Proposal for a Regulation,

laying down Union procedures for the authorisation and supervision of medicinal products for human use and establishing rules governing the European Medicines Agency.

EUROPEAN COMMISSION

Reasons for and objectives of the proposal

EU pharmaceutical legislation has enabled the authorisation of safe, efficacious and high-quality medicinal products. However, patient access to medicinal products across the EU and security of supply are growing concerns, mirrored by recent Council conclusions and resolutions of the European Parliament. (Note: European Parliament resolution of 2 March 2017 on EU options for improving access to medicine (2016/2057(INI), European Parliament resolution of 17 September 2020 on the shortage of medicines (2020/2071(INI)).

There is also a growing problem of shortages of medicinal products for many EU/EEA countries. Consequences of such shortages include decreased quality of treatment received by patients and increased burden on health systems and on healthcare professionals, who need to identify and provide alternative treatments.

While the pharmaceutical legislation creates regulatory incentives for innovation and regulatory tools to support timely authorisation of innovative and promising therapies, these products do not always reach the patient, and patients in the EU have differing levels of access.

Moreover, innovation is not always focused on unmet medical needs, and there are market failures, especially in the development of priority antimicrobials that can help address antimicrobial resistance.

Scientific and technological developments and digitalisation are not fully exploited, while the environmental impact of medicinal products needs attention. In addition, the authorisation system could be simplified to keep up with global regulatory competition.

The pharmaceutical strategy for Europe is a holistic answer to the current challenges of the pharmaceutical policy with legislative and non-legislative actions interacting together to achieve its overall goal of ensuring EU's supply of safe and affordable medicinal products and supporting the EU pharmaceutical industry's innovation efforts.

Reviewing the pharmaceutical legislation is key to achieving these objectives. However, innovation, access and affordability are also influenced by factors outside the scope of this legislation, such as global research and innovation activities or national pricing and reimbursement decisions.

Hence, not all problems can be addressed by the revision of the legislation alone. Despite this, EU pharmaceutical legislation can be an enabling and connecting factor for innovation, access, affordability and environmental protection.

The proposed revision of the EU pharmaceutical legislation builds on the high level of public health protection and harmonisation already achieved for the authorisation of medicinal products. The overarching aim of the reform is to ensure that patients across the EU have timely and equitable access to medicines.

Another objective of the proposal is to enhance security of supply and address shortages through specific measures, including stronger obligations on marketing authorisation holders to notify potential or actual shortages and marketing withdrawals, cessations and suspensions in advance of a foreseen interruption to continued supply of a medicinal product to the market.

To support the sector's global competitiveness and innovative power, right balance needs to be struck between giving incentives for innovation, with more focus on unmet medical needs, and measures on access and affordability. The framework needs to be simplified, adapted to scientific and technological changes, and contribute to reducing the environmental impact of medicinal products.

This proposed reform is comprehensive but targeted and focuses on provisions relevant to achieving its specific objectives; therefore it covers all provisions apart from those concerning advertising, falsified medicinal products, and homeopathic and traditional herbal medicinal products.

To read more:
https://health.ec.europa.eu/system/files/2023-04/com_2023_193_1_act_en.pdf

Number 7

Proposal for a Directive,

on the Union code relating to medicinal products for human use,

The Union general pharmaceutical legislation was established in 1965 with the dual objective of safeguarding public health and harmonising the internal market for medicines.

It has developed considerably since then, but these overarching objectives have guided all revisions. The legislation governs the granting of marketing authorisations for all medicines for human use by defining conditions and procedures to enter and remain on the market.

A fundamental principle is that a marketing authorisation is granted only to medicines with a positive benefit-risk balance after assessment of their quality, safety and efficacy.

The most recent comprehensive revision took place between 2001 and 2004 while targeted revisions on post-authorisation monitoring (pharmacovigilance) and on falsified medicines were adopted subsequently.

In the almost 20 years since the last comprehensive revision, the pharmaceutical sector has changed and has become more globalised, both in terms of development and manufacture.

Moreover, science and technology have evolved at a rapid pace. However, there continues to be unmet medical needs, i.e. diseases without or only with suboptimal treatments.

Moreover, some patients may not benefit from innovation because medicines may be unaffordable or not placed on the market in the Member State concerned.

There is also a greater awareness of the environmental impact of medicines. More recently, the COVID-19 pandemic has stress tested the framework.

This revision is part of the implementation of the Pharmaceutical strategy for Europe and aims to promote innovation, in particular for unmet medical needs, while reducing regulatory burden and the environmental impact of medicines; ensure access to innovative and established medicines

for patients, with special attention to enhancing security of supply and addressing risks of shortages, taking into account the challenges of the smaller markets of the Union; and create a balanced and competitive system that keeps medicines affordable for health systems while rewarding innovation.

This revision focuses on provisions relevant to achieve its specific objectives; therefore it covers all but provisions concerning falsified medicines, homeopathic and traditional herbal medicines.

Nevertheless, for the sake of clarity, it is necessary to replace Directive 2001/83/EC of the European Parliament and of the Council with a new Directive.

The provisions on falsified medicines, homeopathic medicines and traditional herbal medicines are therefore maintained in this Directive without changing their substance compared to previous harmonisations. However, in view of the changes in the governance of the Agency, the Herbal Committee is replaced by a working group.

The essential aim of any rules governing the authorisation, manufacturing, supervision, distribution and use of medicinal products must be to safeguard public health. Such rules should also ensure the free movement of medicinal products and the elimination of obstacles to trade in medicinal products to all patients in the Union.

The regulatory framework for medicinal products use should also take into account the needs of the undertakings in the pharmaceutical sector and trade in medicinal products within the Union, without jeopardising the quality, safety and efficacy of medicinal products.

To read more:
https://health.ec.europa.eu/system/files/2023-04/com_2023_192_1_act_en.pdf

Number 8

Active Cyber Defence (ACD) program - The Sixth Year

Key findings from the 6th year of the ACD program

National Cyber Security Centre

The aim of Active Cyber Defence (ACD) is to "Protect the majority of people in the UK from the majority of the harm caused by the majority of the cyber attacks the majority of the time."

It was launched in 2017 and continues to protect the UK, in a relatively automated way, from a significant proportion of commodity cyber attacks.

National Cyber Security Centre

Active Cyber Defence

The 6th Year: Summary of Key Findings

Web shells

Web shells are created by attackers using malicious scripts to install control panels on compromised servers.

These servers can then be used as a launch pad for malicious activity such as hosting phishing sites. The number of web shells we have discovered and acted against increased in 2022 by around 15%.

The most prevalent hosting providers of web shells were Newfold Digital, Cloudflare and GoDaddy.

Early Warning

www.ncsc.gov.uk/information/early-warning-service

Early Warning is a free NCSC service designed to automatically inform an organisation of potential cyber attacks on their network, as soon as possible.

The service uses a variety of information feeds from the NCSC, and trusted public, commercial and closed sources (which includes several privileged feeds which are not available elsewhere).

Early Warning filters millions of events that the NCSC receives every day and - using the IP and domain names provided by our users - correlates those which are relevant to their organisation into daily notifications for their nominated contacts.

Contents

What is Active Cyber Defence? 3
Takedown Service 4
Suspicious Email Reporting Service (SERS) 7
Mail Check 8
Vulnerability Checking 9
Protective Domain Name Service (PDNS) 10
Exercise in a Box 11
Early Warning 12

To read more:
https://www.ncsc.gov.uk/section/active-cyber-defence/introduction

https://www.ncsc.gov.uk/files/acd6-summary.pdf

Number 9

ESAs call for vigilance in the face of mounting financial risks

The three European Supervisory Authorities (EBA, EIOPA and ESMA - ESAs) issued their Spring 2023 Joint Committee Report on risks and vulnerabilities in the EU financial system.

While noting that EU financial markets remained broadly stable despite the challenging macro environment and recent market pressure in the banking sector, the three Authorities are calling on national supervisors, financial institutions and market participants to remain vigilant in the face of mounting risks.

The second half of 2022 witnessed a worsening of the macro environment due to high inflation and tighter financial conditions, and the economic outlook remains uncertain.

Although recent growth forecasts no longer point to a deep recession and inflation is showing signs of moderation, price growth may remain elevated for longer than previously expected.

Recent market pressure on banks following the collapse of a few midsize banks in the United States and the emergency merger of the distressed Credit Suisse with the Union Bank of Switzerland (UBS) highlighted continued high market uncertainty, the sensitivity of the European financial system to exogenous shocks and potential risks related to the end of over a decade of very low interest rates.

Asset prices were highly volatile over the past months with market liquidity fragile. Sharp movements in prices triggered sizeable margin calls and put some market participants under liquidity strains, notably non-financial corporations and non-bank financial institutions.

High levels of uncertainty and imbalances in the supply and demand of liquidity are a drag on the financial system's resilience against further external shocks. In addition to these risks, geopolitical tensions, environmental threats and an increase in the frequency and sophistication of cyberattacks further complicate the risk landscape.

Against the backdrop of these risks and vulnerabilities, the Joint Committee of the ESAs advises national supervisors, financial institutions and market participants to take the following policy actions:

- financial institutions and supervisors should remain prepared for a deterioration in asset quality and supervisors should keep a close eye on loan loss provisioning;

- the broader impact of policy rate increases and sudden rises in risk premia on financial institutions and market participants should be considered and accounted for in (liquidity) risk management;

- liquidity risks arising from investments in leveraged funds and the use of interest rate derivatives should be monitored closely;

- financial institutions and supervisors should closely monitor the impacts of inflation risk. Inflation can have an impact on asset valuation and asset quality as borrower debt servicing is affected. Inflationary trends should be taken into account in product testing, product monitoring and product review phases and investors should be made aware of the effects of inflation on real returns;

- banks should pursue prudent capital distribution policies to ensure their long-term financial resilience given the uncertain medium-term outlook for profitability;

- the strong regulatory frameworks that underpin the resilience of the financial sector are to be maintained, including by faithfully implementing the finalization of Basel III in the EU without delay and with as little deviation as possible, and by avoiding further deviations from EIOPA's advice on the Solvency II review;

- risk management capabilities and disclosures for environmental, social and governance (ESG) risks should be enhanced as these risks are increasingly becoming a source of financial risk; and

- financial institutions should allocate adequate resources and skills to ensure the security of their information and communication technology (ICT) infrastructures and adequate ICT risk management.

To read more:
https://www.eiopa.europa.eu/esas-call-vigilance-face-mounting-financial-risks-2023-04-25_en

Number 10

Developing Agile, Reliable Sensing Systems with Microbes

DARPA's Tellus program seeks to advance remote environmental sense-and-respond platforms with enhanced breadth, resolution

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Current environmental monitoring approaches can rely on both distributed sensor networks - on the ground or in the water - and remote sensing platforms, like satellites, to collect information important for the protection of people and property.

The Department of Defense (DOD) is interested in developing new, complementary sensors to monitor the environment with high spatial resolution, and reduced power and logistical burden, to further enhance monitoring capabilities and significantly reduce potential risk to personnel.

Recent research has demonstrated that microbes, such as bacteria, fungi, or microalgae, offer promise for detecting different types of input signals, including both chemical (e.g., toxic or radioactive materials, heavy metal pollutants) and physical phenomena (e.g., light, electric current, magnetic fields).

Microbes can also generate both chemical and physical output signals in response to sensing these inputs. The ability to detect and convert signals, be self-powering, and environmental resilience are microbial features that may complement other sensing approaches.

DARPA's new Tellus program will explore the development of an interactive, platform methodology for the rapid design of microbe-based sense-and-respond devices for monitoring DOD-relevant environments.

Specifically, DARPA seeks to establish the range of chemical and physical signals that microbial devices can detect, environmental conditions they can tolerate, and types of output signals that can be generated.

To this end, Tellus will focus on developing the methodology to enable the rapid design of agile, robust, reliable, and durable microbial sensors for environmental monitoring.

The microbial devices developed during the 2.5-year program must be able to translate detected signals into a variety of physical or chemical output signals, including light, non-toxic organic compounds, or electric current, which can then be measurable by conventional receiver systems (e.g., optoelectronic, photonic, imaging, electrode).

In addition to method development, Tellus is focused on assessing sensor functionality across many different environments and conditions. As remote environmental monitoring for chemicals, pollutants, or changing conditions is an area of national security interest, microbial sensing systems that are capable of detecting multiple types input targets, relaying a variety of output signals at a distance, and operating unattended for long durations are desired.

“As part of the program, DARPA will test how quickly new, functional devices can be designed, built, and tested using specific parameters,” stated Dr. Linda Chrisey, Tellus program manager.

“Ultimately, we envision a dashboard or interface where a user would dial in features of their environment, the inputs they want to detect, and the output signals that are useful to them, and the system would design a safe, effective microbial device to meet those needs.”

To read more: https://www.darpa.mil/news-events/2023-04-21

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,

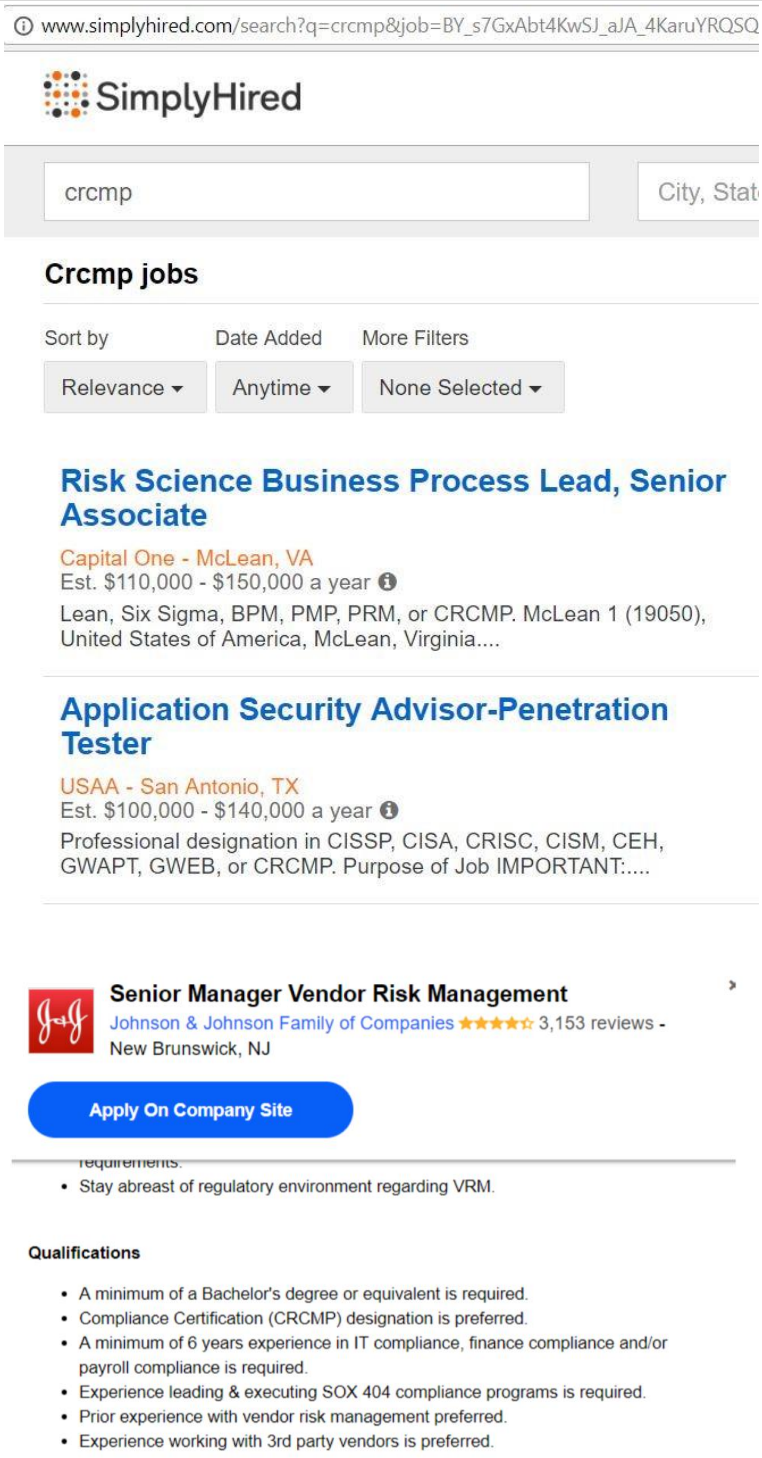
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- 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.