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, December 19, 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,

Can auditors use the work of specialists, such as valuation specialists, appraisers, and actuaries? Of course, they can. Are there any risks in this practice? Of course, there are always risks when we rely on others, experts or not.

According to the Public Company Accounting Oversight Board (PCAOB), a *specialist* is "a person (or firm) possessing special skill or knowledge in a particular field other than accounting or auditing."

The use and importance of specialists has increased in recent years, in part due to the *increasing complexity* of business transactions and the resulting complexity of information needed to account for those transactions. This complexity may contribute to *increased risks* of material misstatement in financial statements.

In 2015, we had a consultation paper, developed by staff of the Office of the Chief Auditor of the PCAOB, that was not a statement of the PCAOB, and had not been approved by the PCAOB.

The paper described a potential *need for changes* to PCAOB standards. According to the paper, the use of the work of specialists was once largely limited to companies in *specialized industries,* such as financial services, oil and gas. In 2015, accounting for business transactions had become more complicated due to elaborate business structures and complex transactions that were difficult to measure.

Financial reporting standards had changed in response to the increased complexity. Since 1995, the Financial Accounting Standards Board ("FASB") had issued standards that increasingly required the use of estimates such as fair value measurements.

Figure 1: Examples of Activities that Involve the Work of Specialists

Activities	Types of Specialists
Valuation	
Assets acquired and liabilities assumed in business combinations	Valuation specialist / appraiser
Complex financial instruments	Valuation specialist
Environmental remediation contingencies	Engineer
Goodwill impairments	Valuation specialist
Insurance reserves	Actuary
Intangible assets	Valuation specialist
Jewelry and art	Appraiser
Pension and other post-employment obligations	Actuary
Real estate	Appraiser
Stock options	Valuation specialist
Evaluation of physical and other characteristics	
Materials stored in stockpiles	Geologist
Mineral reserves and condition	Geologist
Oil and gas reserves	Geologist
Property, plant, and equipment useful lives and salvage values	Valuation specialist / appraiser
Interpretation of laws, regulations, or contracts	
Legal title to property or interpretation of laws, regulations, or contracts	Lawyer

On March 20, 2019, the PCAOB filed with the Securities and Exchange Commission (SEC), pursuant to Section 107(b) of the Sarbanes-Oxley Act, a proposal to *adopt amendments* to auditing standards for auditor's use of

the work of specialists. The SEC found that the proposed rules were consistent with the requirements of the Sarbanes-Oxley Act and the securities laws.

In December 2002, we have another very interesting PCAOB staff white paper, with title "Econometric Analysis on the Initial Implementation of the New Specialists Requirements".

We read that the PCAOB is committed to understanding the initial impact of the new requirements for auditing accounting estimates, including fair value measurements ("Estimates Requirements") and the auditor's use of the work of specialists ("Specialists Requirements").

They performed an econometric analysis to examine pre-post differences in specialist usage and hours associated with the implementation of the new specialists requirements.

Read more at number 4 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)

Share it with your family
Holiday Scams

Number 2 (Page 9)

FX settlement risk: an unsettled issue
Marc Glowka, Thomas Nilsson

Number 3 (Page 11)

Remarks Before the Investor Advisory Committee
SEC Chair Gary Gensler

Number 4 (Page 13)

Post-Implementation Review of AS 2501, Auditing Accounting Estimates, Including Fair Value Measurements; Amendments to Auditing Standards for Auditor's Use of the Work of Specialists

Number 5 (Page 16)

Capacity building in the financial sector in the face of emerging challenges
Mahesh Kumar Jain, Deputy Governor, of the Reserve Bank of India, at the Golden Jubilee celebration function of the National Institute for Banking Studies and Corporate Management (NIBSCOM), Noida.

Number 6 (Page 19)

Frequently asked questions on climate-related financial risks

BIS

Number 7 (Page 22)

DEV-0139 launches targeted attacks against the cryptocurrency industry

Microsoft Security Threat Intelligence

Microsoft

Number 8 (Page 24)

Cyber Europe 2022: After Action Report

Findings from a PAN-EUROPEAN cyber crisis Exercise

enisa
European Network and Information Security Agency

Number 9 (Page 27)

A capability definition and assessment framework for countering disinformation information influence, and foreign interference

Published by the NATO Strategic Communications Centre of Excellence

Number 10 (Page 31)

Molecules Have an Orientation, and Scientists Have a New Way to Measure It

Molecular orientation is key to designing better materials.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Number 1

Share it with your family
Holiday Scams

When shopping online during the holiday season—or any time of year—always be wary of deals that seem too good to be true. Do your part to avoid becoming a scammer's next victim.

Every year, thousands of people become victims of holiday scams. Scammers can rob you of hard-earned money, personal information, and, at the very least, a festive mood.

The two most prevalent of these holiday scams are non-delivery and non-payment crimes. In a non-delivery scam, a buyer pays for goods or services they find online, but those items are never received. Conversely, a non-payment scam involves goods or services being shipped, but the seller is never paid.

According to the Internet Crime Complaint Center's (IC3) 2021 report, non-payment or non-delivery scams cost people more than $337 million. Credit card fraud accounted for another $173 million in losses.

Similar scams to beware of this time of year are auction fraud, where a product is misrepresented on an auction site, and gift card fraud, when a seller asks you to pay with a pre-paid card.

The IC3 receives a large volume of complaints in the early months of each year, suggesting a correlation with the previous holiday season's shopping scams.

Tips to Avoid Holiday Scams

Whether you're the buyer or the seller, there are a number of ways you can protect yourself—and your wallet.

Practice good cybersecurity hygiene.

- Don't click any suspicious links or attachments in emails, on websites, or on social media. Phishing scams and similar crimes get you to click on links and give up personal information like your name, password,

and bank account number. In some cases, you may unknowingly download malware to your device.

- Be especially wary if a company asks you to update your password or account information. Look up the company's phone number on your own and call the company.

Know who you're buying from or selling to.

- Check each website's URL to make sure it's legitimate and secure. A site you're buying from should have https in the web address. If it doesn't, don't enter your information on that site.

- If you're purchasing from a company for the first time, do your research and check reviews.

- Verify the legitimacy of a buyer or seller before moving forward with a purchase. If you're using an online marketplace or auction website, check their feedback rating. Be wary of buyers and sellers with mostly unfavorable feedback ratings or no ratings at all.

- Avoid sellers who act as authorized dealers or factory representatives of popular items in countries where there would be no such deals.

- Be wary of sellers who post an auction or advertisement as if they reside in the U.S., then respond to questions by stating they are out of the country on business, family emergency, or similar reasons.
- Avoid buyers who request their purchase be shipped using a certain method to avoid customs or taxes inside another country.

Be careful how you pay.

- Never wire money directly to a seller.

- Avoid paying for items with pre-paid gift cards. In these scams, a seller will ask you to send them a gift card number and PIN. Instead of using that gift card for your payment, the scammer will steal the funds, and you'll never receive your item.

- Use a credit card when shopping online and check your statement regularly. If you see a suspicious transaction, contact your credit card company to dispute the charge.

Monitor the shipping process.

- Always get tracking numbers for items you buy online, so you can make sure they have been shipped and can follow the delivery process.

- Be suspect of any credit card purchases where the address of the cardholder does not match the shipping address when you are selling. Always receive the cardholder's authorization before shipping any products.

To read more:
https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/holiday-scams

Number 2

FX settlement risk: an unsettled issue

Marc Glowka, Thomas Nilsson

BIS

Key takeaways

- In April 2022, $2.2 trillion of daily FX turnover was subject to settlement risk, up from an estimated $1.9 trillion in April 2019.
- FX settlement risk, the risk that one party in a currency trade fails to deliver the currency owed, remains because existing settlement arrangements to mitigate risk are unavailable, or unsuitable for settling certain trades, or market participants find them too expensive.
- Public and private sector stakeholders are working to reduce FX settlement risk for a broader range of currencies and market participants.

FX settlement risk, the risk that one party to a trade of currencies fails to deliver the currency owed, can result in significant losses for market participants, sometimes with systemic consequences.

The failure of Bankhaus Herstatt in 1974, the best-known example, eroded confidence in interbank relations and caused a freeze in money market lending (Galati (2002)). Recent examples include KfW Bankengruppe's €300 million loss when Lehman Brothers collapsed in 2008 (Hughes (2009)), and Barclays' $130 million loss to a small currency exchange in March 2020 (Parsons (2021)).

Almost 50 years after the Herstatt bankruptcy, nearly a third of deliverable FX turnover remains subject to settlement risk, according to new data from the 2022 BIS Triennial Survey.

While this share is unchanged from the 2019 Survey, settlement risk has increased in absolute terms in line with the growth in FX turnover. That is, $2.2 trillion was at risk on any given day in April 2022, up from an estimated $1.9 trillion in April 2019.

This feature assesses the scale of FX settlement risk and the mechanisms in place to mitigate it.

We first document the current risk level and its components, drawing on expanded FX settlement risk data in the 2022 BIS Triennial Survey.

Second, we highlight the reasons why risk remains.

Third, we present ongoing policy initiatives and private sector innovations to mitigate this risk.

Mechanisms to reduce settlement risk

Market participants have two main options for mitigating FX settlement risk.

First, they can bilaterally offset their payment obligations to reduce the amounts that need to be settled (ie "pre-settlement netting").

Second, they can settle any remaining turnover via payment - versus - payment (PvP) arrangements or via the same clearer, termed "on-us".

In a PvP mechanism, the final payment of one currency occurs if, and only if, the final payment of the other currency takes place.

In on-us settlement, both payment legs settle across the books of a single institution. However, parties are protected against loss only if both legs settle simultaneously or if settlement is certain to occur within preauthorised credit lines (ie "on-us with loss protection").

Pre-settlement netting reduced settlement risk in almost a fifth of deliverable turnover in 2022, unchanged from 2019. As turnover has grown, this amounts to pre-settlement netting of $1.3 trillion per day, up from an estimated $1.1 trillion in 2019.

The increase can be attributed to wider availability of automated netting services, driven also by market pressure to reduce funding costs. In the remaining turnover to be settled, much settlement risk remains despite the broader adoption of PvP arrangements since 1997.

To read more: https://www.bis.org/publ/qtrpdf/r_qt2212i.pdf

Number 3

Remarks Before the Investor Advisory Committee

SEC Chair Gary Gensler

Good morning. Once again, it is good to be back with the Investor Advisory Committee. As is customary, I would like to note that my views are my own and that I am not speaking on behalf of the Commission or SEC staff.

I want to begin by welcoming the Committee's new Access and Inclusion Working Group. Access and inclusion are so important, as they relate directly to fairness in the markets. Fairness, of course, sits within the middle part of the SEC's mission: to maintain fair, orderly, and efficient markets.

Today's Investor Advisory Committee's meeting will cover a range of investor issues through **three** panels.

I understand that your first panel is on account statements, which are important to all investors, especially retail investors. Account statements provide a primary avenue for investors to evaluate how their investments are performing and the costs in their portfolio. I look forward to hearing the panelists' suggestions on how we can enhance these statements and make them more useful for investors.

Second, I understand that you have a panel discussing public companies' disclosure of their taxes. I am glad to see this and look forward to the Committee's discussion, as taxes are an important expense for public companies.

Investors have expressed an interest in greater details, sometimes called disaggregation, with regard to income tax information.

In an effort to make more informed investment decisions, investors have raised an interest in understanding more about tax information related to the specific jurisdictions in which companies operate, including how different tax strategies might impact companies' tax rates.

I understand the Financial Accounting Standards Board (FASB) recently proposed to enhance income tax disclosures in financial statements.

When the proposal is publicly released, I think it is important to consider such enhanced tax disclosures. Disaggregated tax reporting from international companies—in the specific jurisdictions in which those companies operate—could benefit investors.

Finally, I understand you have a panel looking at complex investment products known as single-stock exchange-traded funds (ETFs).

As the SEC's Office of Investor Education and Advocacy said in a statement earlier this year, single-stock ETFs, including levered and/or inverse single-stock ETFs, can present unique risks to investors, especially retail investors.

Holding a single-stock ETF is not the same thing as holding the underlying stock or a traditional ETF. Investing in a levered, single-stock ETF may create exposures for investors that in many ways resemble buying shares on margin.

With respect to inverse single-stock ETFs, investing in them is meant to be similar to shorting a stock.

Though these products are listed or traded on exchanges, they are not necessarily right for every investor.

Further, they often are designed to be held for a short time period, such as a single day.

Thus, I look forward to the panel's discussion on these complex products and steps the SEC might take to advance investor protection in this area.

I wish you a productive meeting and happy holidays.

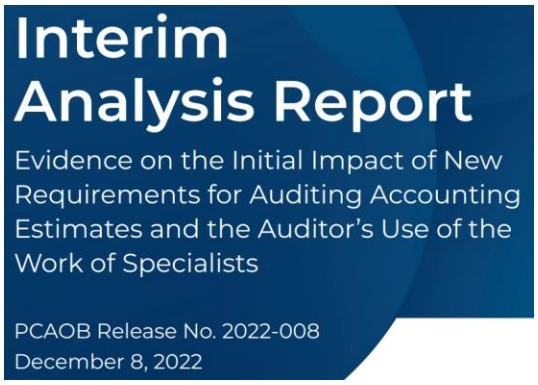
To read more:
https://www.sec.gov/news/speech/gensler-remarks-iac-120822

Number 4

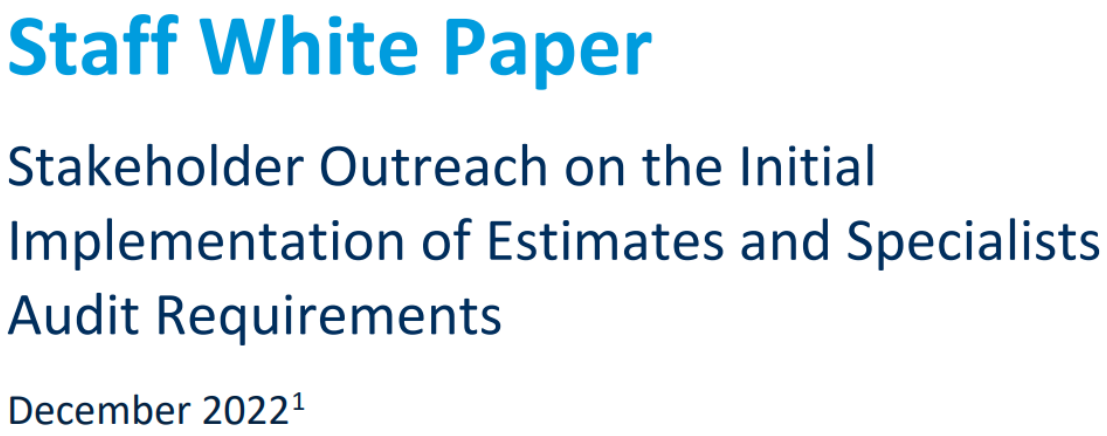
Post-Implementation Review of AS 2501, Auditing Accounting Estimates, Including Fair Value Measurements; Amendments to Auditing Standards for Auditor's Use of the Work of Specialists

The PCAOB has released an interim analysis report and two accompanying staff white papers examining the initial impact of new requirements for auditing accounting estimates, including fair value measurements ("Estimates Requirements") and the auditor's use of the work of specialists ("Specialists Requirements"). Given the identical effective dates and concurrent implementation efforts for these standards, our analysis considered the effects of both standards at once.

1. Interim Analysis Report: Evidence on the Initial Impact of New Requirements for Auditing Accounting Estimates and the Auditor's Use of the Work of Specialists (December 2022)



2. Staff White Paper: Stakeholder Outreach on the Initial Implementation of Estimates and Specialists Audit Requirements (PDF) (December 2022)



3. Staff White Paper: Econometric Analysis on the Initial Implementation of the New Specialists Requirements (PDF) (December 2022)

Staff White Paper

Econometric Analysis on the Initial Implementation of the New Specialists Requirements

December 2022[1]

To inform the analysis, the staff of the PCAOB's Office of Economic and Risk Analysis surveyed audit firms; interviewed audit engagement partners, audit committee chairs, and preparers; analyzed the comment letters received through a public request for comment on initial experiences with implementing the new requirements; and conducted large-sample statistical analysis.

Staff also evaluated whether evidence gathered on initial implementation of the Estimates Requirements and Specialists Requirements is suggestive of significant benefits, costs, or unintended consequences.

Key findings from the staff's analyses include the following:

- About one-third of the audit firms in the staff's survey reported that the new requirements improved auditing practices. Other audit firms reporting that the effects of the new standard were limited and generally asserted that their prior policies and methodologies were already largely aligned with the new requirements.

- Audit firms had significant variation in the amount of time they spent to support implementation of the new requirements and in training firm personnel for these new requirements.

- At the audit engagement level, almost all audit firms and audit engagement partners reported that the new requirements did not result in significant increases in audit hours or audit fees.

- Statistical analysis of PCAOB inspections data finds evidence of changes in specialist usage following implementation of the Specialists

Requirements.

- The staff has not found evidence of significant unintended consequences or implementation challenges associated with the new requirements.

The Board will continue to monitor the implementation of the new requirements and their impact on the quality of audit services, as well as on audit committees, preparers, and audit firms.

Further information on the implementation of the new requirements for auditing accounting estimates and using the work of specialists as audit evidence is available in the Standards section of this website.

To read more:
https://pcaobus.org/oversight/standards/pir/post-implementation-review-as2501-auditing-accounting-estimates-fair-value-measurements-auditors-use-work-specialists

Number 5

Capacity building in the financial sector in the face of emerging challenges

Mahesh Kumar Jain, Deputy Governor, of the Reserve Bank of India, at the Golden Jubilee celebration function of the National Institute for Banking Studies and Corporate Management (NIBSCOM), Noida.

1. Thank you for inviting me to the Golden Jubilee celebration of this premier institution. Over the last 50 years the National Institute for Banking Studies and Corporate Management (NIBSCOM) has provided exemplary service to the banking industry by training several generations of bankers in operational and management aspects relating to banking and finance.

I am given to understand that since inception, there have been around 2 lakh participants in its training programmes. Having started my banking career with Punjab National Bank, one of the sponsor banks of NIBSCOM, I am specially delighted to be here amongst you.

2. In addition to various statutory and regulatory requirements, banking also has certain time-honoured banking conventions and practices. These practical concepts are best understood by practitioners and therefore best taught by them too.

Moreover, unlike other professions such as medical, legal or accounting where there are specific academic courses, bankers come from a wide variety of academic backgrounds and learn their craft on the job.

Therefore, industry promoted capacity building institutions like NIBSCOM play a crucial role in developing and enhancing the skills of bankers. Apart from sharing mutual experiences, this collaboration also helps in optimizing training costs.

3. Recognising the importance of capacity building, the Reserve Bank has catalysed the establishment of several institutions, both for upskilling of its own staff as well as of the industry. These include Reserve Bank Staff College, College of Agricultural Banking (CAB), Indira Gandhi Institute of Development Research (IGIDR), Institute for Development and Research in Banking Technology (IDRBT), National Institute of Bank Management

(NIBM), Indian Institute of Bank Management (IIBM), Centre for Advanced Financial Research and Learning (CAFRAL), RBI Academy and more recently College of Supervisors.

4. Today, I would like to talk to you about the learnings from the challenges faced by financial sector in the last decade, the emerging challenges and the importance of capacity building in this context.

A decade of challenges

5. The last decade has been exceptionally challenging for banks and financial institutions in India. In December 2011, the Financial Stability Report first highlighted the rising NPA levels. Subsequently, Central Repository of Information on Large Credits (CRILC), introduced in 2013 and AQR in 2015 revealed the scale of NPA problem.

As the banking sector was working towards remedying the situation, the IL&FS default in 2018, revealed cracks in the liquidity management of NBFCs. This was followed by a spate of problematic episodes like DHFL, Punjab & Maharashtra Co-operative Bank, Yes Bank, LVB and ultimately the Covid-19 pandemic.

6. The Covid-19 pandemic is a watershed event of our generation for the widespread devastation of life and livelihood that it caused. It still haunts the global economy in several ways. There are very few parallels of a shock like COVID-19 in history, which left policymakers with no template to navigate through the crisis.

7. Before I continue, I would like to express my gratitude and appreciation for the bankers and RBI staff for their dedicated service during the pandemic. Even at the risk to their lives, bankers ensured that branches remain open and functional.

Teams in the RBI and its regulated entities ensured availability of critical support infrastructure for payment settlement systems, ATMs, internet/ mobile banking, dealing with cyber security risks, address the customer grievances, etc. so that banking services continued uninterrupted.

8. As you all know, RBI's monetary policy mandate is to maintain price stability while keeping in mind the objective of growth. In response to the COVID-19 pandemic, the Monetary Policy Committee prioritised growth adopting an accommodative stance necessary to revive and sustain growth on a durable basis and mitigate the impact of COVID-19 on the economy. The RBI implemented a slew of measures, both conventional and

unconventional, to address the pandemic-induced dislocations and constraints.

9. In terms of conventional measures, the policy repo rate was reduced significantly. Further, system-level liquidity was also enhanced through large-scale open market purchase operations and a one percentage point reduction in the cash reserve ratio.

Unconventional measures such as long-term repo operations (LTRO), targeted long-term repo operations (LTRO) and special open market operations (Operation Twist) were also conducted to support growth. Most importantly, the liquidity was closely monitored and to avoid falling into a liquidity trap, all the RBI liquidity measures came with sunset clauses.

To read more:
https://www.rbi.org.in/scripts/FS_Speeches.aspx?Id=1342&fn=2

Number 6

Frequently asked questions on climate-related financial risks

BIS

This standard has been integrated into the consolidated Basel Framework.

The Basel Committee on Banking Supervision issued responses to frequently asked questions (FAQs) to clarify how climate-related financial risks may be captured in the existing Basel Framework.

These FAQs intend to facilitate a globally consistent interpretation of existing Pillar 1 standards given the unique features of climate-related financial risks and should not be interpreted as changes to the standards.

This publication is part of the Committee's holistic approach to addressing climate-related financial risks to the global banking system.

The responses are consistent with the Basel Committee's Principles for the effective management and supervision of climate-related financial risks. You may visit: https://www.bis.org/bcbs/publ/d532.pdf

FAQ 7

To what extent should banks consider climate-related financial risks when determining property value?

Answer

Banks should determine whether the current market value incorporates the potential changes in the value of properties emerging from climate-related financial risks (eg potential damage related to weather hazards, the implementation of climate-policy standards or changes in investment and consumption patterns derived from transition policies). National supervisors should consider jurisdiction-specific features that account for climate-related financial risks when setting out prudent valuation criteria.

Introduction

The Basel Framework is the full set of standards of the Basel Committee on Banking Supervision, the primary global standard setter for the prudential regulation of banks.

To help promote consistent interpretation of the framework, the Basel Committee periodically publishes the answers to frequently asked questions (FAQs).

This document sets out a number of FAQs that the Basel Committee has agreed to add to the Basel Framework covering issues related to climate-related financial risks.

The Basel Committee is taking a holistic approach to addressing climate-related financial risks to the global banking system in support of its mandate to strengthen the regulation, supervision and practices of banks worldwide with the purpose of enhancing financial stability.

In pursuing this work, the Basel Committee is examining the extent to which climate-related financial risks can be addressed within the Basel Framework, identifying potential gaps in the current framework and considering possible measures to address them.

Current work in this area is comprehensive in nature, spanning regulatory, supervisory and disclosure dimensions.

In 2021, the Basel Committee published analytical reports that concluded climate risk drivers can be captured in traditional financial risk categories.

For that reason, banks should consider how to incorporate climate-related financial risks in their interpretation and application of the existing Basel Framework, and continuously develop their capacity and expertise in relation to climate-related financial risks.

As part of its holistic approach, the Basel Committee has developed responses to FAQs to clarify how climate-related financial risks may be captured in existing Pillar 1 standards.

Consistent with the objective of FAQs, the responses are intended to facilitate consistent interpretation of existing standards given the unique features of climate-related financial risks and should not be interpreted as changes to the standards.

The responses are consistent with the Basel Committee's Principles for the effective management and supervision of climate-related financial risks (2022). Where appropriate, the responses explicitly acknowledge data limitations and recognise practices will evolve iteratively over time.

Given that challenges arising from methodological and data limitations cannot be fully resolved at this time, the responses are intended to allow for flexibility while also encouraging banks to continuously develop their measurement and mitigation of climate-related financial risks and therefore promote a globally consistent implementation of the Basel Framework.

The current publication represents a set of responses to initial FAQs but should not be considered an exhaustive list of standards where the impact of climate risk drivers should be considered.

The Basel Committee will publish additional FAQs in future, as needed, to facilitate implementation of the existing Basel Framework, particularly as the availability of sufficiently granular data and consistent measurement methodologies for climate-related financial risks improves over time.

To read more: https://www.bis.org/bcbs/publ/d543.pdf

Number 7

DEV-0139 launches targeted attacks against the cryptocurrency industry

Microsoft Security Threat Intelligence

Microsoft

Over the past several years, the cryptocurrency market has considerably expanded, gaining the interest of investors and threat actors.

Cryptocurrency itself has been used by cybercriminals for their operations, notably for ransom payment in ransomware attacks, but we have also observed threat actors directly targeting organizations within the cryptocurrency industry for financial gain.

Attacks targeting this market have taken many forms, including fraud, vulnerability exploitation, fake applications, and usage of info stealers, as attackers attempt to get their hands on cryptocurrency funds.

We are also seeing more complex attacks wherein the threat actor shows great knowledge and preparation, taking steps to gain their target's trust before deploying payloads.

For example, Microsoft recently investigated an attack where the threat actor, tracked as DEV-0139, took advantage of Telegram chat groups to target cryptocurrency investment companies.

DEV-0139 joined Telegram groups used to facilitate communication between VIP clients and cryptocurrency exchange platforms and identified their target from among the members.

The threat actor posed as representatives of another cryptocurrency investment company, and in October 2022 invited the target to a different chat group and pretended to ask for feedback on the fee structure used by cryptocurrency exchange platforms.

The threat actor had a broader knowledge of this specific part of the industry, indicating that they were well prepared and aware of the current challenge the targeted companies may have.

After gaining the target's trust, DEV-0139 then sent a weaponized Excel file with the name OKX Binance & Huobi VIP fee comparision.xls which contained several tables about fee structures among cryptocurrency exchange companies.

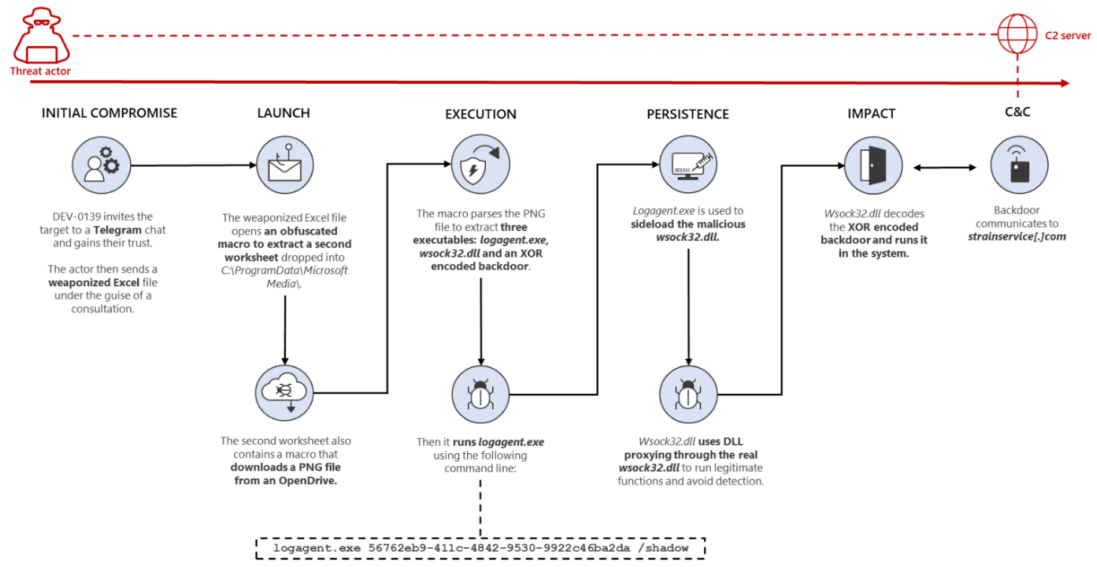


Figure 1. Overview of the attack

The data in the document was likely accurate to increase their credibility. This weaponized Excel file initiates the following series of activities:

1. A malicious macro in the weaponized Excel file abuses UserForm of VBA to obfuscate the code and retrieve some data.

2. The malicious macro drops another Excel sheet embedded in the form and executes it in invisible mode. The said Excel sheet is encoded in base64, and dropped into C:\ProgramData\Microsoft Media\ with the name VSDB688.tmp

3. The file VSDB688.tmp downloads a PNG file containing three executables: a legitimate Windows file named logagent.exe, a malicious version of the DLL wsock32.dll, and an XOR encoded backdoor.

4. The file logagent.exe is used to sideload the malicious wsock32.dll, which acts as a DLL proxy to the legitimate wsock32.dll. The malicious DLL file is used to load and decrypt the XOR encoded backdoor that lets the threat actor remotely access the infected system. To read more: https://www.microsoft.com/en-us/security/blog/2022/12/06/dev-0139-launches-targeted-attacks-against-the-cryptocurrency-industry/

Number 8

Cyber Europe 2022: After Action Report

Findings from a PAN-EUROPEAN cyber crisis Exercise

Cyber Europe is a series of EU-level cyber incident and crisis management exercises organised by ENISA. It is aimed at both the public and private sectors from the EU and EFTA Member States.

The exercises simulate large-scale cybersecurity incidents that escalate into cyber crises, offering opportunities to analyse advanced technical cybersecurity incidents but also test participants on their capabilities for dealing with complex situations.

The exercises aim to test the participants' readiness and capacity to tackle challenging and realistic cyber crises.

The exercises are organised by ENISA together with planners from participating countries and institutions. Cyber Europe 2022 aimed to accomplish several Goals and Objectives which are detailed below.

Cyber Europe 2022 was designed to fulfil a list of Goals (G). These Goals were developed to provide the organisers and the participants with a clear scope and a purpose for their participation in the event.

The 2022 edition aimed to achieve the following Goals:

G1. Test EU-level technical and operational cooperation during cyber-crises,

G2. Provide opportunities to test local-level incident response and resilience plans,

G3. Train EU- and local-level technical capabilities.

These Goals were complemented by the following secondary (also known as implicit) Goals:

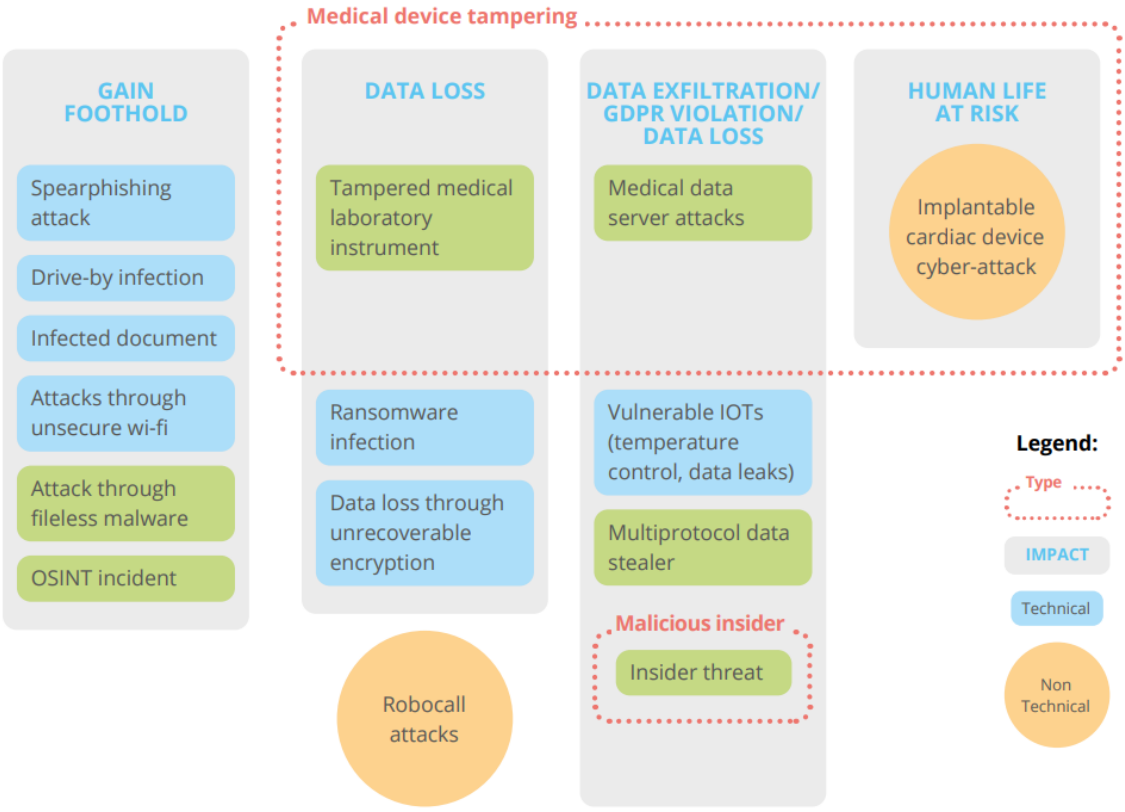
- Help to build trust
- Engage the private sector
- Improve situational awareness
- Test the public affairs response
- Improve the exercise's process and capabilities.

Cyber Europe 2022 revolved around the healthcare ecosystem and tested the resilience of several relevant stakeholders, including national Computer Security Incident Response Teams (CSIRTs), cybersecurity authorities, ministries of health, healthcare organisations such as hospitals and clinics, eHealth service providers, and health insurance providers.

The participants had to address an escalating cyber crisis, tackling multiple incidents simultaneously. The scenario aimed at realistically mimicking technical incidents.

These incidents are detailed in Figure 1 below, which highlight how they covered several elements, with some aimed at gaining a foothold and others aimed at tampering with medical devices.

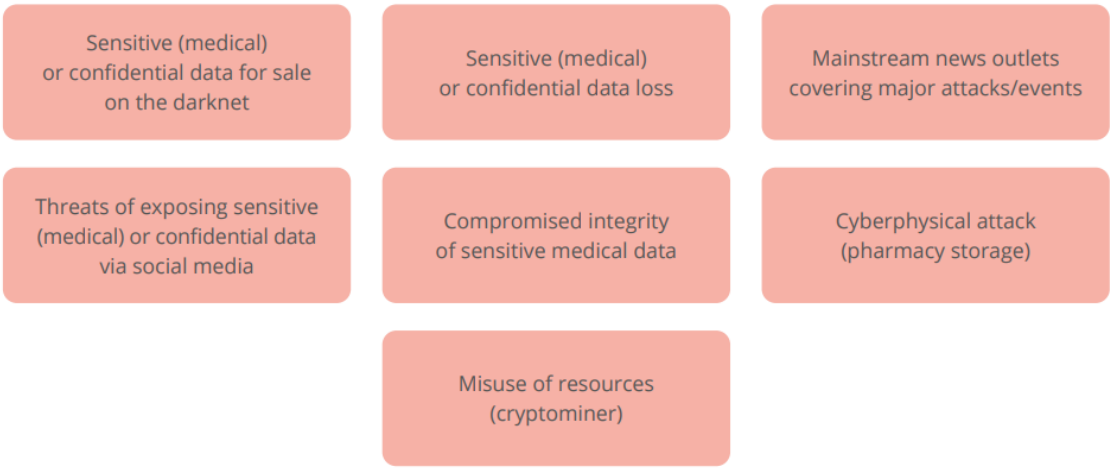
Figure 1. Overview of the technical scenario



The second figure describes the sectors targeted by the attacks and their potential impacts.

The objective of the scenario was to enable the players to react accordingly to each incident in order to minimise the damage incurred, with the general objective of testing the operational and technical layers.

Figure 2. Targeted sectors and potential impact of the attacks



The scenario, which spanned two days, began on the first day by engaging the participants around a disinformation campaign of manipulated laboratory results and a cyberattack targeting the networks of European hospitals as well as internet and cloud service providers.

To read more:
https://www.enisa.europa.eu/publications/cyber-europe-2022-after-action-report

Number 9

A capability definition and assessment framework for countering disinformation information influence, and foreign interference

Published by the NATO Strategic Communications Centre of Excellence

This report proposes a capability assessment framework for countering disinformation, information influence, and foreign interference.

At present, much emphasis is placed on the capability to counter disinformation and other associated phenomena. However, few have attempted to systematically define what those countermeasures are, and how they could be placed within a single, coherent capability assessment framework.

This lack is not least because countries do not, and should not, approach these challenges in the same way.

Geography, history, political systems, areas of expertise, and relative power explain to some extent why countries use different terminologies, organisational structures, and policies for dealing with foreign interference.

Furthermore, friendly actors at times share capabilities–such as tech platforms, researchers, non-governmental organisations (NGOs), and private-sector intelligence companies.

There is no perfect template for assessing capabilities, but rather only organisations and systems designed to cope with different threats based on their mandates, interests, and available resources.

Since there is no one-size-fits-all solution to this problem, this report provides a flexible approach to capability assessment based on simple principles that can be applied by different types of actors.

In support of this, and drawing upon previous research in this subject area, four capability assessment tools are established as tools to solve different assessment problems:

1. Objectives are a cluster of capability measures associated with the explicit or implied purpose of an activity. Assessment can be developed, for example, from policy announcements, norms and expectations, and archetypical examples.

2. Indicators weigh the factors that contribute to objectives, deconstructing them into constituent parts.

Assessment can be developed, for example, from qualitative and quantitative measures, subjective and objective data, as well as from process measures such as response time, throughput, or success rate.

3. Risk assessments prioritise anticipated vulnerabilities and threats and can help to assess preparedness for those scenarios.

4. Process maturity assesses organisational and process efficiency on a scale that begins with ad hoc and unstructured practices and ends with highly optimised routines.

The capability assessment framework proposed in this report takes this toolset and applies it in three stages.

First, disinformation, information influence, and foreign interference are defined. In the order shown, these three terms represent an escalating scale of breadth and strategic intent.

Briefly, their generally accepted definitions are as follows:

1. Disinformation refers to a group of activities where the intent and factualness of message content is in focus.

2. Information influence refers to manipulative communication techniques used in support of an actor's goals.

3. Foreign interference refers to efforts to achieve a hostile foreign actor's goals using hybrid methods including disinformation and/or information influence.

Second, these definitions are used to establish a basis for categorising countermeasures. Countermeasures are grouped into overall approaches and broken down into specific capabilities.

Each group of countermeasures consists of several individual capabilities; in total, around 50 unique capabilities are defined according to this schema.

1. Disinformation's main countermeasures involve the capability to determine and correct the factualness of messages (correcting content) and capabilities relevant to improving public resilience to misinformation and questionable sources.

2. The main countermeasures for information influence involve more advanced analysis and identification capabilities as well as proactive strategic communication capabilities designed to push back on covert campaigns.

3. The main countermeasures for foreign interference involve intelligence and security policy capabilities that are honed to deal with communicative threats.

4. In addition, a further group of capabilities are included to cover system-wide questions, such as capabilities distributed across a country-wide system, shared capabilities within partnerships and alliances, as well as staff development capabilities.

The third layer of the framework provides general indications regarding which assessment methods from the aforementioned toolset are most applicable to each group of capabilities.

Examples are suggested in a way that demonstrates the overall applicability of tools to different assessment challenges, rather than attempting to define a single solution.

In most cases, a combination of two or more assessment tools will be relevant to most organisations.

The importance of taking steps toward a viable capability assessment framework should not be understated.

Currently, there is much talk of a need for Counter-foreign interference capabilities at the political level, with limited efforts to understand how to assess and develop those capabilities at the level of individual tasks, at the scale of country systems, within formal and informal alliances, or for prioritised threat scenarios.

The framework proposed here offers a modest step forward, without overly prescribing how assessment should be used, given the sensitivity of national differences.

Different types of organisations, including government departments and agencies, local government, NGOs, research organisations,

intergovernmental alliances, tech companies, private-sector intelligence companies, and other stakeholders, can take inspiration from this framework to design a tailored schema for comparative capability assessment.

To read more:
https://stratcomcoe.org/publications/a-capability-definition-and-assessment-framework-for-countering-disinformation-information-influence-and-foreign-interference/255

Number 10

Molecules Have an Orientation, and Scientists Have a New Way to Measure It

Molecular orientation is key to designing better materials.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

In some materials, the molecules line up in a regular, repeating pattern. In others, they all point in random directions. But in many advanced materials used in medicine, computer chip manufacturing and other industries, the molecules arrange themselves in complex patterns that dictate the material's properties.

Scientists haven't had good ways to measure molecular orientation in three dimensions at a microscopic scale, leaving them in the dark about why some materials behave the way they do.

Now, researchers at the National Institute of Standards and Technology (NIST) have measured the 3D orientation of the molecular building blocks of plastics, called polymers, observing details as small as 400 nanometers, or billionths of a meter, in size.

The measurements, described in the Journal of the American Chemical Society, show polymer chains twisting and undulating in complex and unexpected ways. The new measurements were made using a souped-up version of a technique called broadband coherent anti-Stokes Raman scattering, or BCARS.

BCARS works by shining laser beams at a material, causing its molecules to vibrate and emit their own light in response. This technique, developed about a decade ago at NIST, is used to identify what a material is made of.

To measure molecular orientation, NIST research chemist Young Jong Lee has added a system for controlling the polarization of the laser light and new mathematical methods for interpreting the BCARS signal.

Specifically, the new technique measures the average orientation of the polymer chains within 400-nanometer regions, along with the distribution of orientations around that average.

These measurements will allow scientists to identify molecular orientation patterns that produce the mechanical, optical and electrical properties they seek.

“Understanding that structure/function relationship can really speed up the discovery process,” Lee said.

This will help researchers to optimize the materials used in medical devices such as arterial stents and artificial knees. The orientation of the molecules on the surface of those devices helps determine how well they bond with muscle, bone and other tissues.

It can also help with additive manufacturing, in which products are fabricated by 3D-printing them, layer upon layer — a technique that is transforming the electronics, automotive, aerospace and other industries.

3D printing often uses polymers, and researchers are constantly seeking new ones with better strength, flexibility, heat resistance and other properties.

The new measurement technique might also be used to optimize the polymer-based ultrathin films used in semiconductor manufacturing.

As the components within computer chips get smaller and smaller — as Moore’s law predicts they will — the molecular orientations in those films become increasingly important.

To read more:
https://www.nist.gov/news-events/news/2022/12/molecules-have-orientation-and-scientists-have-new-way-measure-it

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,

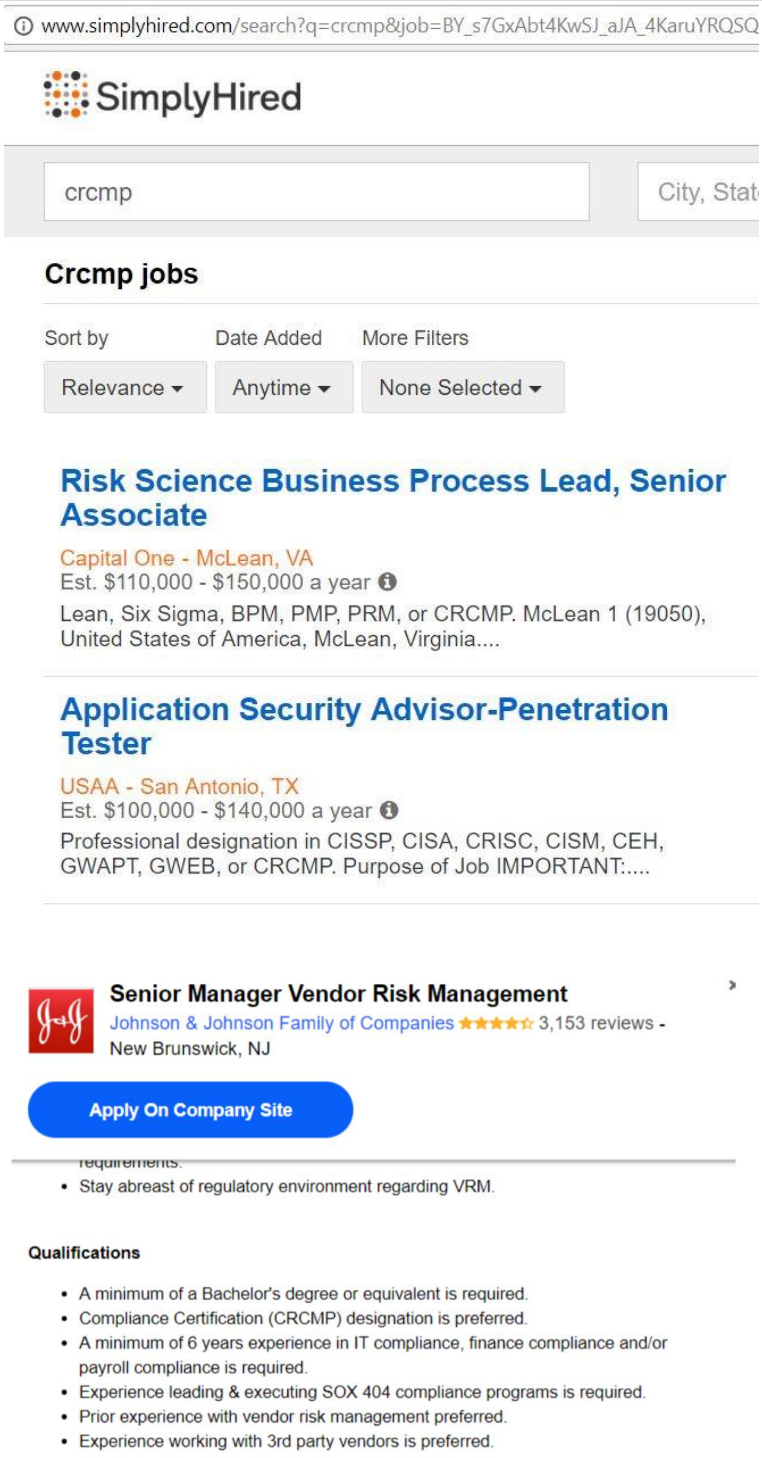
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- 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.