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, January 23, 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,

We expect a surprise for *auditors* from the European Commission. I was reading the final text of the EU Digital Operational Resilience Act (DORA) - (EU) 2022/2554. In Article 58 we read that by 17 January 2026, the European Commission shall carry out a review and submit a report to the European Parliament and the Council, accompanied, where appropriate, by a legislative proposal.

Which is the scope of the review? The appropriateness of *strengthened requirements for statutory auditors and audit firms as regards digital operational resilience,* by means of the *inclusion* of statutory auditors and audit firms into the scope of this Regulation, or by means of amendments to Directive 2006/43/EC of the European Parliament and of the Council.

Directive 2006/43/EC is the 8th Company Law Directive, it is also called ESOX, the European Sarbanes-Oxley.

The Digital Operational Resilience Act (DORA) is a very interesting regulation. Before DORA, financial institutions managed the main categories of financial risk (credit risk, market risk, liquidity risk etc.) using the traditional quantitative approach (setting a capital requirement), but they did not manage all components of operational resilience.

After the Russia's invasion of Ukraine that, according to Ursula von der Leyen, president of the European Commission, has brought death, devastation and unspeakable suffering, and after DORA, financial institutions must also follow qualitative rules for the protection, detection, containment, recovery and repair after ICT-related incidents.

DORA explicitly refers to ICT risk and sets rules on ICT risk-management, incident reporting, operational resilience testing and ICT third-party risk monitoring. This Regulation acknowledges that ICT incidents and a lack of operational resilience have the possibility to jeopardise the soundness of the financial system, even if there is "adequate" capital for the traditional risk categories in individual institutions.

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

Best regards,

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

Number 1 (Page 5)

Preparing the economy and financial system for hybrid war - Finland's experience

Olli Rehn, Governor of the Bank of Finland, at the Peterson Institute for International Economics (PIIE) Financial Statements web event series

Number 2 (Page 7)

The EU Digital Operational Resilience Act (DORA)

Number 3 (Page 10)

Costs and past performance report 2023

Number 4 (Page 14)

Irving Fisher Committee on Central Bank Statistics

Number 5 (Page 17)

Pilot Climate Scenario Analysis Exercise

Participant Instructions, January 2023

Number 6 (Page 21)

Why Bank Capital Matters

Board of Governors of the Federal Reserve System, Vice Chair for Supervision Michael S. Barr, at the American Enterprise Institute, Washington, D.C.

Number 7 (Page 23)

Interoperable EU Risk Management Framework

Number 8 (Page 25)

XLLing in Excel - threat actors using malicious add-ins

By Vanja Svajcer, Cisco Talos Intelligence Blog

Number 9 (Page 27)

CISA Releases Four Industrial Control Systems Advisories

Number 10 (Page 28)

Some paragraphs from the EU Artificial Intelligence Act

Not the final text – It is the proposal from the Council of the European Union for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

Number 1

Preparing the economy and financial system for hybrid war - Finland's experience

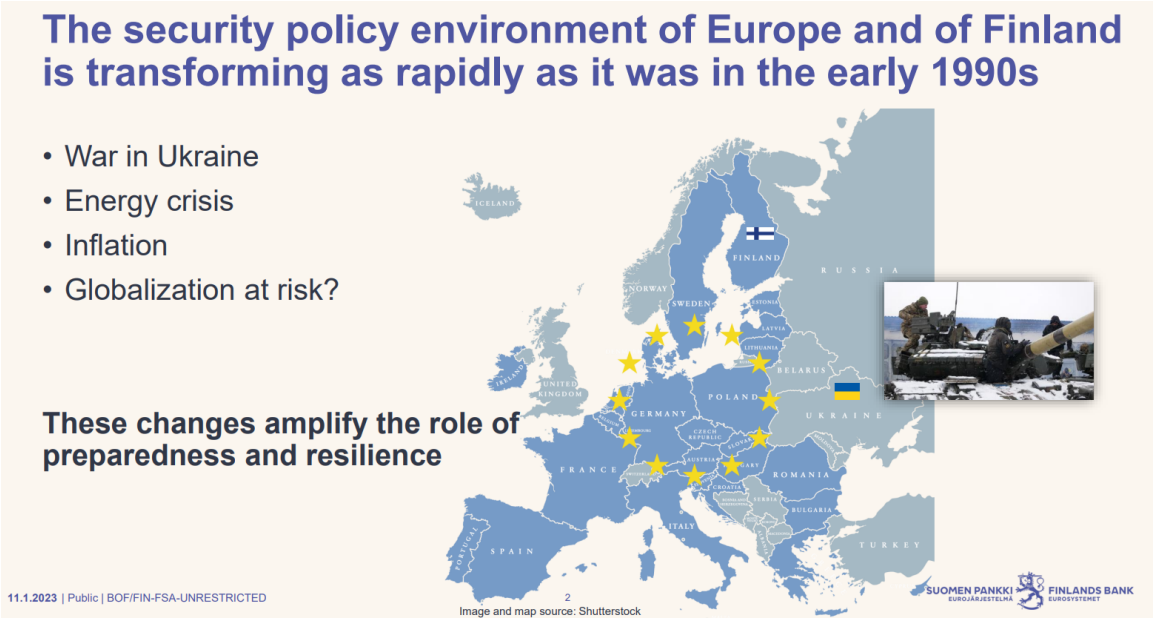
Olli Rehn, Governor of the Bank of Finland, at the Peterson Institute for International Economics (PIIE) Financial Statements web event series

Ladies and Gentlemen,

Greetings from a snowy Helsinki – and thank you very much for this opportunity to exchange views with you at this event today. The topic of my talk is Finland's experience in building up resilience and preparing the economy and financial system to cope with hybrid warfare.

Around a year ago, a rapid recovery from the COVID-19 pandemic was well under way in Europe. Those positive prospects were crushed last February by Russia's illegal and brutal attack against Ukraine.

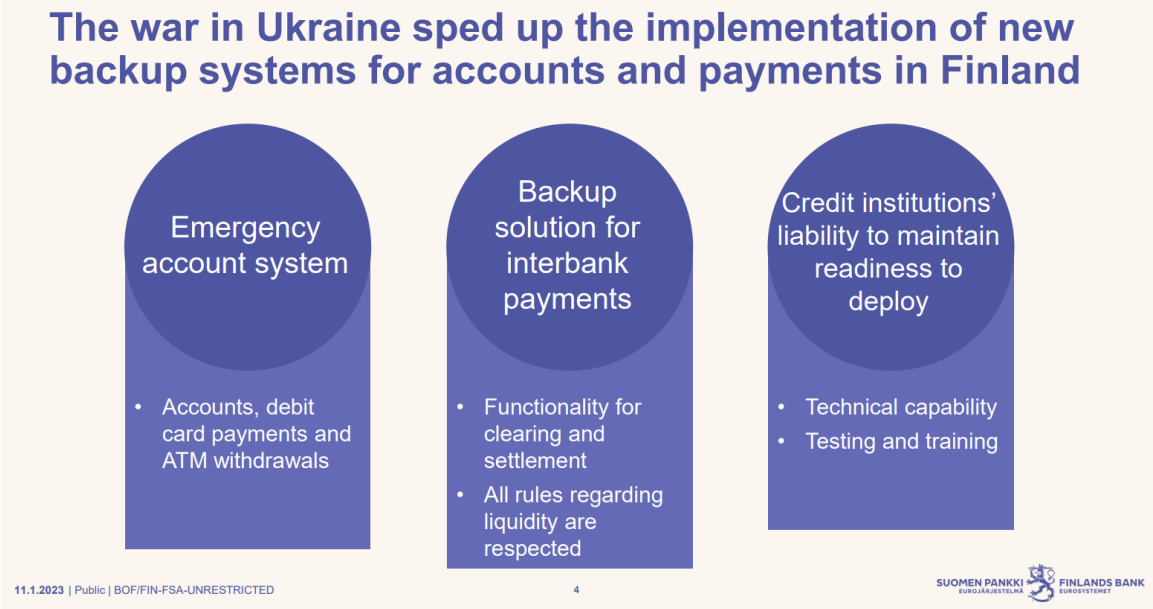
The horrific bombardment of critical Ukrainian infrastructure has left millions of Ukrainians at the mercy of winter conditions, and no end to the war is in sight.



We need to be prepared for a long confrontation between Putin's Russia and the liberal West, or more broadly between authoritarian governments and liberal democracies.

Russia's war has been a litmus test of European unity. Supporting Ukraine in its fight for freedom remains a policy priority. For Finns, this is really close to our hearts, also by our own experience.

After all, we ourselves were attacked by the Soviet Union in the Second World War, and we still have Europe's longest border with Russia: 832 miles, or 1340 kilometres.



To read more:
https://www.suomenpankki.fi/en/media-and-publications/speeches-and-interviews/2023/governor-olli-rehn-preparing-the-economy-and-financial-system-for-hybrid-war-finlands-experience/

SUOMEN PANKKI EUROJÄRJESTELMÄ FINLANDS BANK EUROSYSTEMET

Number 2

The EU Digital Operational Resilience Act (DORA)

EUR-Lex
Access to European Union law

Article 1, Subject matter

1. In order to achieve a high common level of digital operational resilience, this Regulation lays down uniform requirements concerning the security of network and information systems supporting the business processes of financial entities as follows:

(a) requirements applicable to financial entities in relation to:

(i) information and communication technology (ICT) risk management;

(ii) reporting of major ICT-related incidents and notifying, on a voluntary basis, significant cyber threats to the competent authorities;

(iii) reporting of major operational or security payment-related incidents to the competent authorities by financial entities referred to in Article 2(1), points (a) to (d);

(iv) digital operational resilience testing;

(v) information and intelligence sharing in relation to cyber threats and vulnerabilities;

(vi) measures for the sound management of ICT third-party risk;

(b) requirements in relation to the contractual arrangements concluded between ICT third-party service providers and financial entities;

(c) rules for the establishment and conduct of the Oversight Framework for critical ICT third-party service providers when providing services to financial entities;

(d) rules on cooperation among competent authorities, and rules on supervision and enforcement by competent authorities in relation to all matters covered by this Regulation.

2. In relation to financial entities identified as essential or important entities pursuant to national rules transposing Article 3 of Directive (EU) 2022/2555, this Regulation shall be considered a sector-specific Union legal act for the purposes of Article 4 of that Directive.

3. This Regulation is without prejudice to the responsibility of Member States' regarding essential State functions concerning public security, defence and national security in accordance with Union law.

Article 2, Scope

1. Without prejudice to paragraphs 3 and 4, this Regulation applies to the following entities:

(a) credit institutions;

(b) payment institutions, including payment institutions exempted pursuant to Directive (EU) 2015/2366;

(c) account information service providers;

(d) electronic money institutions, including electronic money institutions exempted pursuant to Directive 2009/110/EC;

(e) investment firms;

(f) crypto-asset service providers as authorised under a Regulation of the European Parliament and of the Council on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 ('the Regulation on markets in crypto-assets') and issuers of asset-referenced tokens;

(g) central securities depositories;

(h) central counterparties;

(i) trading venues;

(j) trade repositories;

(k) managers of alternative investment funds;

(l) management companies;

(m) data reporting service providers;

(n) insurance and reinsurance undertakings;

(o) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries;

(p) institutions for occupational retirement provision;

(q) credit rating agencies;

(r) administrators of critical benchmarks;

(s) crowdfunding service providers;

(t) securitisation repositories;

(u) ICT third-party service providers.

2. For the purposes of this Regulation, entities referred to in paragraph 1, points (a) to (t), shall collectively be referred to as 'financial entities'.

3. This Regulation does not apply to:

(a) managers of alternative investment funds as referred to in Article 3(2) of Directive 2011/61/EU;

(b) insurance and reinsurance undertakings as referred to in Article 4 of Directive 2009/138/EC;

(c) institutions for occupational retirement provision which operate pension schemes which together do not have more than 15 members in total;

(d) natural or legal persons exempted pursuant to Articles 2 and 3 of Directive 2014/65/EU;

(e) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries which are microenterprises or small or medium-sized enterprises;

(f) post office giro institutions as referred to in Article 2(5), point (3), of Directive 2013/36/EU.

4. Member States may exclude from the scope of this Regulation entities referred to in Article 2(5), points (4) to (23), of Directive 2013/36/EU that are located within their respective territories. Where a Member State makes use of such option, it shall inform the Commission thereof as well as of any subsequent changes thereto. The Commission shall make that information publicly available on its website or other easily accessible means.

To read more: https://eur-lex.europa.eu/eli/reg/2022/2554/oj

Number 3

Costs and past performance report 2023

EIOPA Costs and Past Performance Report provides an overview of the (past) performance and costs of EU retail investment products within EIOPA's remit.

The coverage period goes from 2017 to year end 2021 for past performance and 2021 for costs.

Past performance has been positively influenced by the post-COVID recovery which led to markets achieving high results in 2021.

Performance results have been affected by the initial market turbulence at the on-set of the COVID-19 crisis, the significant market recovery of end 2020 and early 2021 followed by the on-set of the inflationary pressures, market turbulence and more conservative growth outlooks, which emerged at the end of 2021.

This is expected to continue throughout 2022.

While the latter issues are only captured to a limited extent, given that up to year-end 2021 inflation did not raise significantly and the markets downturn was not significant, some considerations have been included, particularly given the outlook and expected results for 2022.

In 2021, EIOPA achieved its coverage target. The sample collected comprised of:

▪ More than 1000 insurance-based investment products (IBIPs), marketed by 170 undertakings, accounting for a total of € 171.6 billion Gross Written Premium (GWP), which represents around 78% of the total EEA GWP for the unit-linked and with profit participation lines of business;

▪ More than 200 personal pension products (PPPs), accounting for a total of 1.7 million contracts and for a total of € billion 36.2 GWP;

▪ More than 162 thousand schemes offered by more than 1400 Institutions for Occupational Retirement provision (IORPs), holding more than 2.5 trillion assets under management.

In 2021, IBIPs offered positive returns, with unit-linked (UL) products delivering an average return – based on the sample collected – of 9.4%, hybrid (HY) products an average return – based on the sample collected – of 4.0% and profit participation (PP) products – based on the sample collected – an average return of 1.3%.

The different performance should be read in conjunction with the intrinsic differences of the products.

The performance reported for unit-linked products is due to exceptionally high market performance.

In fact, unit-linked products by exposing consumers directly to market trends are subjected to higher volatility.

Meaning that, unlike profit participation and hybrid product which offer some protection to consumers, when markets underperform these products also expose consumers to significantly higher risk of losses – e.g. in 2018, as reported in the 2020 EIOPA's Cost and Past Performance Report, UL products reported a -7% loss, HY products a -2% loss while PP products had a positive (2.3%) return.

The net performance of IBIPs is also influenced by the risk class, recommended holding period (RHP) and, to a lesser extent, by the premium frequency.

The risk class is the most significant driver for UL products' performance: higher risk classes deliver higher levels of net return in times of high market performance, while in times of market turbulence they generally expose consumers to higher losses.

The RHP weights more for PP products, with longer holding periods to drive higher net returns.

Costs have, generally, remained stable, with PP products continuing to be cheaper than UL and HY products despite a cost decrease for UL products.

Despite the decrease in the reduction in yield (RIY) for UL products (-5 bps), these continue to be more expensive than PP products, whose average RIY in 2021 stood at 1.6%.

Hybrid have similar levels of costs as UL products (2.3%). Ongoing costs continue being the major component driving the total RIY, but the different treatment of costs across countries hinders comparability.

While improvements have been observed, in some cases cost-structures continue to be complex and opaque, in particular for multi-option products, highlighting the need for further supervisory and regulatory interventions.

The appetite for sustainable products is rapidly growing as also indicated in EIOPA's 2022 Consumer Trends Report.

Moreover, while the sample is still limited and conclusions should be drawn carefully, in 2021 products with sustainability features (ESG-products) appear to have performed better than products with no sustainability features.

UL products defined with sustainability features, as self-reported by insurance undertakings, provided higher returns for investors in 2021, while being overall cheaper than products which have not been classified as having sustainability features.

UL products with sustainability features delivered net returns of 11.2%, against 9.4% from their non-ESG peers. UL products with sustainability features, reported an average RIY of 2.1%, while the non-ESG peers reported 2.3%.

Such outcome does not hold for HY products as HY products with sustainability features delivered net returns of 3.2%, against 4.0% from their non-ESG peers.

For PP products only a negligible number of products was reported as having sustainability features.

It is important to note however that the Taxonomy Regulation did not enter into force in 2021 and so the above mentioned are first tentative considerations based on undertakings' own classification.

This year's report also provides information on selected products which are sold on a cross-border basis: they seem to have, on average, higher costs, particularly for UL products, than the ones sold within the home market.

The reason could be higher distribution costs linked to the need of establish distribution networks.

These high-level conclusions could also be driven by the limited sample of products collected.

In fact, EIOPA asked to provide information for products sold on a cross-border basis for those Member States which write 50% or more of

GWP on a cross-border basis, and this only accounts for 33.1% of total GWP written on a cross-border basis.

To read more:
https://www.eiopa.europa.eu/sites/default/files/publications/reports/costs_and_past_performance_report_2023_0.pdf

Number 4

Irving Fisher Committee on Central Bank Statistics

On 9 January 2023 the BIS All Governors' meeting approved the publication of the 2022 Annual Report of the Irving Fisher Committee on Central Bank Statistics (IFC).

It provides a brief update on the IFC's governance and a review of its main workstreams, including planned initiatives.

Members of the IFC Executive as of January 2023

Executive member	Institution	Term
Pablo García (Chair)	Central Bank of Chile	2022–25[2]
Yakubu Aminu Bello	Central Bank of Nigeria	2021–25
Elizabeth Holmquist	Board of Governors of the Federal Reserve System	2022–24
Robert Kirchner	Deutsche Bundesbank	2020-25
Ko Nakayama	Bank of Japan	2020–24
Li Ming Ong	Central Bank of Malaysia	2020–23
Gloria Peña	Central Bank of Chile	2019–24
Fernando Alberto Rocha	Central Bank of Brazil	2018–24
Eyal Rozen	Bank of Israel	2021–23
Silke Stapel-Weber	European Central Bank	2019–24
Luís Teles Dias	Banco de Portugal	2022–24

Executive summary

As a global network that discusses and develops statistical issues of interest to central banks, the IFC now has 98 members and is an affiliated member of the International Statistical Institute (ISI).

It is chaired by Pablo García, Vice Governor of the Central Bank of Chile. One notable feature last year was the decision to host the central bank network on historical monetary and financial statistics (HMFS) under the IFC umbrella.

This group brings together central bank statisticians and academic experts to focus on long-run historic monetary and financial data that are relevant to policymakers.

Another important development for the Committee was related to the international cooperation framework under the Data Gaps Initiative (DGI) endorsed by the G20.

The IFC has continued to actively support the remaining work decided in response to the Great Financial Crisis (GFC) of 2007–09 and to help to coordinate national work on financial data sets.

It is also contributing to the new phase of the DGI initiated in 2022 that calls for better data to understand climate change, income and wealth, financial innovation and inclusion, and access to private and administrative data and data-sharing, to make official statistics more detailed and timely.

In addition, IFC member central banks and the BIS have been actively participating in the ongoing revision of the international statistical manuals (covering the System of National Accounts (SNA) and balance of payments (BPM)) and supporting the global legal entity identification (LEI) system and the Statistical Data and Metadata eXchange standard (SDMX).

The main areas covered by the IFC last year, thanks to the support of its member central banks, the ISI and a number of international organisations, centred on:

• *Post-pandemic landscape for central bank statistics:* the Committee continued to update its web page for Covid-19 statistical resources, which details related official projects and relevant experiences. Moreover, the IFC 11th biennial Conference held in August 2022 was an opportunity to reflect on the new normal for official statistics looking forward.

• *Managing (big) data:* the IFC furthered its analyses of the use of big data in central banks and on the contribution that machine learning (ML) in particular can make. In addition, the Committee has set up recurrent workshops on “Data science in central banking” to review developments in the big data ecosystem and the ongoing adoption of data analytics.

• *Governance of official statistics including communication issues:* the Committee has promoted the establishment of strong data governance standards and co-organised with Banco de Portugal a conference focusing on communication in official statistics.

• *Fintech:* IFC work has continued to document how fintech is transforming the financial landscape, creating a number of challenges for statisticians. The Committee also participated in the related global consultation on the revised structure of the International Standard Industrial Classification.

• *Sustainable finance:* the IFC has launched a number of initiatives on sustainable finance, including a publication in 2022 on the development of statistics in the environmental, social and governance (ESG) area.

In 2023, the IFC will continue to promote knowledge-sharing and international cooperation on statistics-related methodologies, initiatives and training, reflecting the important role played by central banks in the production of official statistics.

To this end, the eBIS-restricted network on statistical methodological issues has been complemented by the launch of a dedicated public IFC knowledge centre webpage that includes guidance notes and related methodological and training information.

In addition, the Committee will further its work in the various areas outlined above, and a number of events will be organised in this context with the support of the central banks of Canada, Italy and South Africa. A major one will be the ISI's 64th biennial World Statistics Congress (WSC) in Canada.

To read more: https://www.bis.org/ifc/publ/ifc_ar2022.pdf

Number 5

Pilot Climate Scenario Analysis Exercise

Participant Instructions, January 2023

Executive Summary

The Board is conducting a pilot CSA exercise to learn about large banking organizations' climate risk-management practices and challenges and to enhance the ability of both large banking organizations and supervisors to identify, measure, monitor, and manage climate-related financial risks.

To accomplish these objectives, the Board designed the pilot CSA exercise to gather qualitative and quantitative information about the climate risk-management practices of large banking organizations.

Over the course of the exercise, the Board will engage with participants to understand their approaches and challenges with respect to the financial risks of climate change.

Information collected and discussed with participants will include detailed documentation of governance and risk-management practices, measurement methodologies, data challenges and limitations, estimates of the potential impact on specific portfolios, and lessons learned from this exercise that could inform any future CSA exercises.

The pilot CSA exercise comprises two separate and independent modules: a physical risk module and a transition risk module.

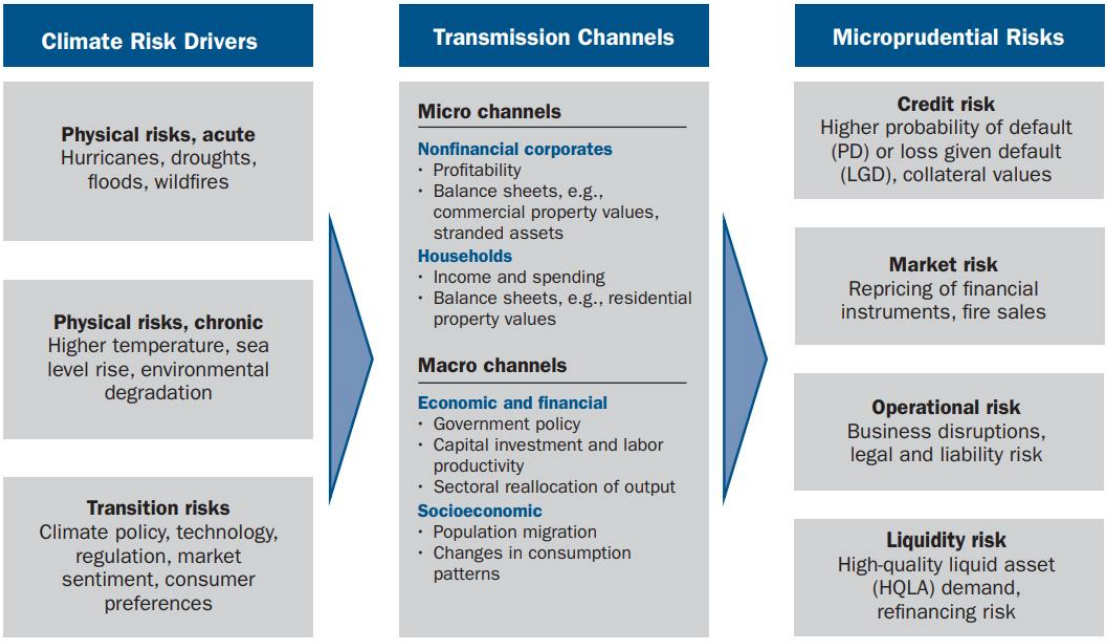
Physical risks represent the harm to people and property that may result from climate-related events, while transition risks represent stresses that may result from the transition to a lower carbon economy.

Both can manifest as traditional prudential risks for large banking organizations.

For both the physical and transition risk modules, the Board will describe forward-looking scenarios to participating large banking organizations, including core climate, economic, and financial variables, where appropriate.

Figure 1. Climate risk drivers manifest as prudential risks

Climate risk drivers could bring about microprudential risks to supervised financial institutions. These risks may manifest through a variety of transmission channels.



Note: Examples are indicative and not exhaustive.

In selecting scenarios for this exercise, the Board leveraged existing work conducted by the Intergovernmental Panel on Climate Change (IPCC) and the Network of Central Banks and Supervisors for Greening the Financial System (NGFS).

The climate scenarios used in the CSA exercise are neither forecasts nor policy prescriptions. They do not necessarily represent the most likely future outcomes or a comprehensive set of possible outcomes.

Rather, the pilot CSA exercise includes a range of plausible future outcomes that can help build understanding of how certain climate-related financial risks could manifest for large banking organizations and how these risks may differ from the past.

Participants will estimate the effect of these scenarios on a relevant subset of their loan portfolios over a future time horizon.

For each loan, participants will calculate and report to the Board credit risk parameters, such as probability of default (PD), internal risk rating grade (RRG), and loss given default (LGD), as appropriate.

Participants will respond to qualitative questions describing their governance, risk-management practices, measurement methodologies, results for specific portfolios, and lessons learned.

Focusing on changes to risk metrics like PD, RRG, and LGD, rather than on estimates of losses, will provide information about how the relative riskiness of exposures within participants' credit portfolios may evolve over time in response to different climate scenarios.

Loss estimates would involve additional assumptions around the evolution of participants' balance sheets and business models and would be incomplete given the partial nature of the exercise, which focuses on specific regions and certain portfolios for six participants.

Six U.S. bank holding companies (BHCs) will participate in this pilot exercise: Bank of America Corporation; Citigroup Inc.; The Goldman Sachs Group, Inc.; JPMorgan Chase & Co.; Morgan Stanley; and Wells Fargo & Company.

These six banking organizations will submit completed data templates, supporting documentation, and responses to qualitative questions to the Federal Reserve Board by July 31, 2023. The Board anticipates publishing insights gained from this pilot exercise around the end of 2023.

The Board expects to disclose aggregated information about how large banking organizations are incorporating climate-related financial risks into their existing risk-management frameworks.

Consistent with the objectives and design of the pilot exercise, the Board does not plan to disclose quantitative estimates of potential losses resulting from the scenarios included in the pilot exercise. No firm-specific information will be released.

This pilot CSA exercise will support the Board's responsibilities to ensure that supervised institutions are appropriately managing all material risks, including financial risks related to climate change.

To read more:
https://www.federalreserve.gov/publications/files/csa-instructions-20230117.pdf

Pilot Climate Scenario Analysis Exercise

Participant Instructions

January 2023

Number 6

Why Bank Capital Matters

Board of Governors of the Federal Reserve System, Vice Chair for Supervision Michael S. Barr, at the American Enterprise Institute, Washington, D.C.

In my first speech as Vice Chair for Supervision in September, I said that the Federal Reserve Board would soon engage in a holistic review of capital standards. My argument, then and now, is that our review of regulatory policy must be a periodic feature of bank oversight.

Banking and the financial system continuously evolve, and regulation must adapt to address emerging risks.

Bank capital is strong, but in doing our review, we should and are being humble about our ability—or that of bank managers—to predict how a future financial crisis might unfold, how losses might be incurred, and what the effect might be on the financial system and our broader economy.

That humility, that skepticism, will serve us well in crafting a capital framework that is enduring and effective. It will help make sure that we do not lose the hard-fought gains in resilience over the past decade and that we prepare for the future.

That review is still underway, and I have no firm conclusions to announce today. Rather, I thought it would be helpful at this early stage to offer my views on capital regulation and the role that capital standards play in helping to advance the safety and soundness of banks and the stability of the financial system.

By "holistic," I mean not looking only at each of the individual parts of capital standards, but also at how those parts may interact with each other—as well as other regulatory requirements—and what their cumulative effect is on safety and soundness and risks to the financial system.

This is not an easy task, because finance is a complex system. And to make the task even harder, we are looking not only at how capital standards are

working today, but also how they may work in the future, when conditions are different.

As I mentioned, we are approaching the task with humility—not with the illusion that there is an immutable capital framework to be discovered, but rather, with the awareness that revisions we conceive of today will reflect our current understanding and will inevitably require updating as our understanding evolves.

To read more:
https://www.federalreserve.gov/newsevents/speech/barr20221201a.htm

Watch live:
https://www.aei.org/events/assessing-the-federal-reserves-capital-framework-a-conversation-with-federal-reserve-vice-chair-michael-barr/

Number 7

Interoperable EU Risk Management Framework

This report is an update of the report “Interoperable EU Risk Management Framework” published by ENISA in January 2022.

The “Interoperable EU Risk Management Framework” proposes a methodology for assessing the potential interoperability of risk management (RM) frameworks and methods and presents related results.

The methods included in this report have been selected as prominent, based on their interoperability features, after evaluating an extended list of risk management frameworks and methods (included in the Compendium of Risk Management Frameworks with Potential Interoperability, ENISA, January 2002) which has been published as Supplement to the Interoperable EU Risk Management.

The “Interoperable EU Risk Management Framework” describes and evaluates the interoperability features for prominent risk management frameworks and methods, by employing a four-level scale to evaluate their interoperability level.

The features assessed to evaluate the interoperability level include the approach used by the RM method (i.e. to whether it is assetbased or scenario-based), whether risk assessment is quantitative or qualitative, as well as other characteristics such as the use of asset taxonomies, valuation methods, the cataloguing of threats and vulnerabilities, the method of risk calculation etc. It also provides an overview of possible collaborative combinations between them.

Characteristics	Parameters to Check
Asset Taxonomy	Does the framework or methodology use or describe specific categories of assets?
	Is the taxonomy used modifiable?
	Can the analyst introduce new categories of assets or import taxonomies from other sources?
Asset Valuation	Does the framework or methodology use or describe specific guidelines for the valuation of assets (i.e. scale and criteria for assessment of asset value and impact)?
	Are the proposed scales or criteria modifiable?
	Can the analyst introduce new scales or criteria?

Characteristics	Parameters to Check
Threat Catalogues	Does the framework or methodology use or describe specific threat catalogues and/or threat categories?
	Are the proposed threat catalogues and/or threat categories modifiable?
	Can the analyst introduce new threats and/or threat categories and import them from other sources?
Vulnerability Catalogues	Does the framework or methodology describe specific vulnerability catalogues and/or categories of vulnerabilities?
	Are the proposed vulnerability catalogues and/or categories of vulnerabilities modifiable?
	Can the analyst introduce new vulnerabilities and/or categories of vulnerabilities and import them from other sources?
Risk Calculation	Does the framework or methodology describe specific guidelines for the calculation of risk (i.e. formulas, scale, matrix)?
	Is the proposed calculation method modifiable?
	Can the analyst introduce or import (from other sources) new methods of calculation?
Measure Catalogues & Calculation of Residual Risk	Does the framework or methodology describe specific control catalogues and/or categories of controls?
	Are the proposed control catalogues and/or categories of controls modifiable?
	Can the analyst introduce new controls and/or categories of controls and import them from other sources?
	Is the Calculation of Residual Risk (either on a Calculation of Residual Risk formula or on an Impact of Measures formula) modifiable?

To read more:
https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework

Number 8

XLLing in Excel - threat actors using malicious add-ins

By Vanja Svajcer, Cisco Talos Intelligence Blog

- Microsoft is phasing out support for executing VBA macros in downloaded Office documents.

- Cisco Talos investigates another vector for introduction of malicious code to Microsoft Excel—malicious add-ins, specifically XLL files.

- Although XLL files were supported since early versions of Excel, including Excel 97, malicious actors started using it relatively recently.

- Currently, a significant number of advanced persistent threat actors and commodity malware families are using XLLs as an infection vector and this number continues to grow.

For decades, Microsoft Office applications have served as one of the most significant entry points for malicious code. Malicious actors have continued to utilize Visual Basic for Applications (VBA) macros, despite automatic warnings to users after opening Office documents containing code.

In addition to VBA macros, malicious actors, from cybercrime actors to state-sponsored groups, also exploited vulnerabilities in Office applications in order to launch malicious code without user intervention.

Over the years, ever since the first VBA malware was discovered at the end of the century, the cybersecurity community have been vocal in calling on Microsoft to introduce default behavior that will block execution of VBA macros if a document was downloaded or received from the internet.

Finally, this year in July, Microsoft started rolling out versions of Office applications which will block execution of any VBA macros by default.

The Office applications now go through a decision making process that is much stricter than before and do not even offer the user a possibility to run macros when a document has a so called Mark Of The Web (MOTW) tag, an alternate data stream that indicates a file has been downloaded from the internet.

Microsoft Office is the most popular office application package used by a large number of corporate and home users with many versions, licensed and unlicensed, still in use worldwide.

Although the change to block macros and not allow their execution through the Office application user interface will be a significant factor in the future, it will take a long time until old versions of Office–still capable of executing macros–are phased out.

Even if malicious actors continue targeting VBA macros in older Office versions, more and more high profile targets will start using new versions which will prevent attacks using documents containing VBA code.

Unfortunately, it would be naive to assume that Office will stop being targeted, now that VBA macros have been blocked. The purpose of this research is to identify other means of introducing third party code into Office applications which, perhaps, are already being used by malware authors.

To read more:
https://blog.talosintelligence.com/xlling-in-excel-malicious-add-ins/

Number 9

CISA Releases Four Industrial Control Systems Advisories

There are 4 very important Industrial Control Systems (ICS) advisories from the U.S. Cybersecurity and Infrastructure Security Agency (CISA) for security flaws affecting products from Siemens, GE Digital, and Contec.

1. Vendor: GE Digital.
Equipment: Proficy Historian.
Exploitable remotely/low attack complexity.
Vulnerabilities: Authentication Bypass using an Alternate Path or Channel, Unrestricted Upload of File with Dangerous Type, Improper Access Control, Weak Encoding for Password.

2. Vendor: Mitsubishi Electric.
Equipment: MELSEC iQ-F and iQ-R Series products.
Exploitable remotely.
Vulnerability: Predictable Seed in Pseudo-Random Number Generator (PRNG).

3. Vendor: Siemens.
Equipment: SINEC INS.
Exploitable remotely/low attack complexity.
Vulnerabilities: OS Command Injection, Inadequate Encryption Strength, Out-of-bounds Write, HTTP Request Smuggling, Inadequate Encryption Strength, Use of Insufficiently Random Values, Authentication Bypass by Spoofing, Path Traversal, Command Injection

4. Vendor: Contec
Equipment: CONPROSYS HMI System (CHS)
Exploitable remotely/low attack complexity.
Vulnerability: OS Command Injection, Use of Default Credentials, Use of Password Hash Instead of Password for Authentication, Cross-site Scripting, Improper Access Control.

To read more:
https://www.cisa.gov/uscert/ncas/current-activity/2023/01/17/cisa-releases-four-industrial-control-systems-advisories

Number 10

Some paragraphs from the EU Artificial Intelligence Act

Not the final text – It is the proposal from the Council of the European Union for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

(8) The notion of remote biometric identification system as used in this Regulation should be defined functionally, as an AI system intended for the identification of natural persons typically at a distance, without their active involvement, through the comparison of a person's biometric data with the biometric data contained in a reference data repository, irrespectively of the particular technology, processes or types of biometric data used.

Such remote biometric identification systems are typically used to perceive (scan) multiple persons or their behaviour simultaneously in order to facilitate significantly the identification of a number of persons without their active involvement.

Such a definition excludes verification / authentication systems whose sole purpose would be to confirm that a specific natural person is the person he or she claims to be, as well as systems that are used to confirm the identity of a natural person for the sole purpose of having access to a service, a device or premises.

This exclusion is justified by the fact that such systems are likely to have a minor impact on fundamental rights of natural persons compared to remote biometric identification systems which may be used for the processing of the biometric data of a large number of persons.

In the case of 'real-time' systems, the capturing of the biometric data, the comparison and the identification occur all instantaneously, near-instantaneously or in any event without a significant delay. In this regard, there should be no scope for circumventing the rules of this Regulation on the 'real-time' use of the AI systems in question by providing for minor delays.

'Real-time' systems involve the use of 'live' or 'near-'live' material, such as video footage, generated by a camera or other device with similar functionality. In the case of 'post' systems, in contrast, the biometric data have already been captured and the comparison and identification occur only after a significant delay. This involves material, such as pictures or video footage generated by closed circuit television cameras or private

devices, which has been generated before the use of the system in respect of the natural persons concerned.

(11) In light of their digital nature, certain AI systems should fall within the scope of this Regulation even when they are neither placed on the market, nor put into service, nor used in the Union.

This is the case for example of an operator established in the Union that contracts certain services to an operator established outside the Union in relation to an activity to be performed by an AI system that would qualify as high-risk. In those circumstances, the AI system used by the operator outside the Union could process data lawfully collected in and transferred from the Union, and provide to the contracting operator in the Union the output of that AI system resulting from that processing, without that AI system being placed on the market, put into service or used in the Union.

To prevent the circumvention of this Regulation and to ensure an effective protection of natural persons located in the Union, this Regulation should also apply to providers and users of AI systems that are established in a **third country,** to the extent the output produced by those systems is used in the Union.

Nonetheless, to take into account existing arrangements and special needs for future cooperation with foreign partners with whom information and evidence is exchanged, this Regulation should not apply to public authorities of a third country and international organisations when acting in the framework of international agreements concluded at national or European level for law enforcement and judicial cooperation with the Union or with its Member States.

Such agreements have been concluded bilaterally between Member States and third countries or between the European Union, Europol and other EU agencies and third countries and international organisations. Recipient Member States authorities and Union institutions, offices, bodies and bodies making use of such outputs in the Union remain accountable to ensure their use comply with Union law.

When those international agreements are revised or new ones are concluded in the future, the contracting parties should undertake the utmost effort to align those agreements with the requirements of this Regulation.

(18) The use of AI systems for ‘real-time’ remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement is considered particularly intrusive in the rights and freedoms

of the concerned persons, to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights.

In addition, the immediacy of the impact and the limited opportunities for further checks or corrections in relation to the use of such systems operating in 'real-time' carry heightened risks for the rights and freedoms of the persons that are concerned by law enforcement activities.

(37) Another area in which the use of AI systems deserves special consideration is the access to and enjoyment of certain essential private and public services and benefits necessary for people to fully participate in society or to improve one's standard of living.

In particular, AI systems used to evaluate the credit score or creditworthiness of natural persons should be classified as high-risk AI systems, since they determine those persons' access to financial resources or essential services such as housing, electricity, and telecommunication services.

AI systems used for this purpose may lead to discrimination of persons or groups and perpetuate historical patterns of discrimination, for example based on racial or ethnic origins, disabilities, age, sexual orientation, or create new forms of discriminatory impacts.

Considering the very limited scale of the impact and the available alternatives on the market, it is appropriate to exempt AI systems for the purpose of creditworthiness assessment and credit scoring when put into service by micro or small entreprises, as defined in the Annex of Commission Recommendation 2003/361/EC for their own use.

Natural persons applying for or receiving essential public assistance benefits and services from public authorities are typically dependent on those benefits and services and in a vulnerable position in relation to the responsible authorities.

If AI systems are used for determining whether such benefits and services should be denied, reduced, revoked or reclaimed by authorities, including whether beneficiaries are legitimately entitled to such benefits or services, those systems may have a significant impact on persons' livelihood and may infringe their fundamental rights, such as the right to social protection, non-discrimination, human dignity or an effective remedy.

Those systems should therefore be classified as high-risk. Nonetheless, this Regulation should not hamper the development and use of innovative approaches in the public administration, which would stand to benefit from a wider use of compliant and safe AI systems, provided that those systems do not entail a high risk to legal and natural persons.

Finally, AI systems used to dispatch or establish priority in the dispatching of emergency first response services should also be classified as high-risk since they make decisions in very critical situations for the life and health of persons and their property.

AI systems are also increasingly used for risk assessment in relation to natural persons and pricing in the case of life and health insurance which, if not duly designed, developed and used, can lead to serious consequences for people's life and health, including financial exclusion and discrimination.

To ensure a consistent approach within the financial services sector, the above mentioned exception for micro or small enterprises for their own use should apply, insofar as they themselves provide and put into service an AI system for the purpose of selling their own insurance products.

38) Actions by law enforcement authorities involving certain uses of AI systems are characterised by a significant degree of power imbalance and may lead to surveillance, arrest or deprivation of a natural person's liberty as well as other adverse impacts on fundamental rights guaranteed in the Charter.

In particular, if the AI system is not trained with high quality data, does not meet adequate requirements in terms of its accuracy or robustness, or is not properly designed and tested before being put on the market or otherwise put into service, it may single out people in a discriminatory or otherwise incorrect or unjust manner.

Furthermore, the exercise of important procedural fundamental rights, such as the right to an effective remedy and to a fair trial as well as the right of defence and the presumption of innocence, could be hampered, in particular, where such AI systems are not sufficiently transparent, explainable and documented.

It is therefore appropriate to classify as high-risk a number of AI systems intended to be used in the law enforcement context where accuracy, reliability and transparency is particularly important to avoid adverse impacts, retain public trust and ensure accountability and effective redress.

In view of the nature of the activities in question and the risks relating thereto, those high-risk AI systems should include in particular AI systems intended to be used by law enforcement authorities for individual risk assessments, polygraphs and similar tools or to detect the emotional state of natural person, for the evaluation of the reliability of evidence in criminal proceedings, for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons, or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups, for profiling in the course of detection, investigation or prosecution of criminal offences.

AI systems specifically intended to be used for administrative proceedings by tax and customs authorities as well as by financial intelligence units carrying out adminstrative tasks analysing information pursuant to Union anti-money laundering legislation should not be considered high-risk AI systems used by law enforcement authorities for the purposes of prevention, detection, investigation and prosecution of criminal offences.

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,

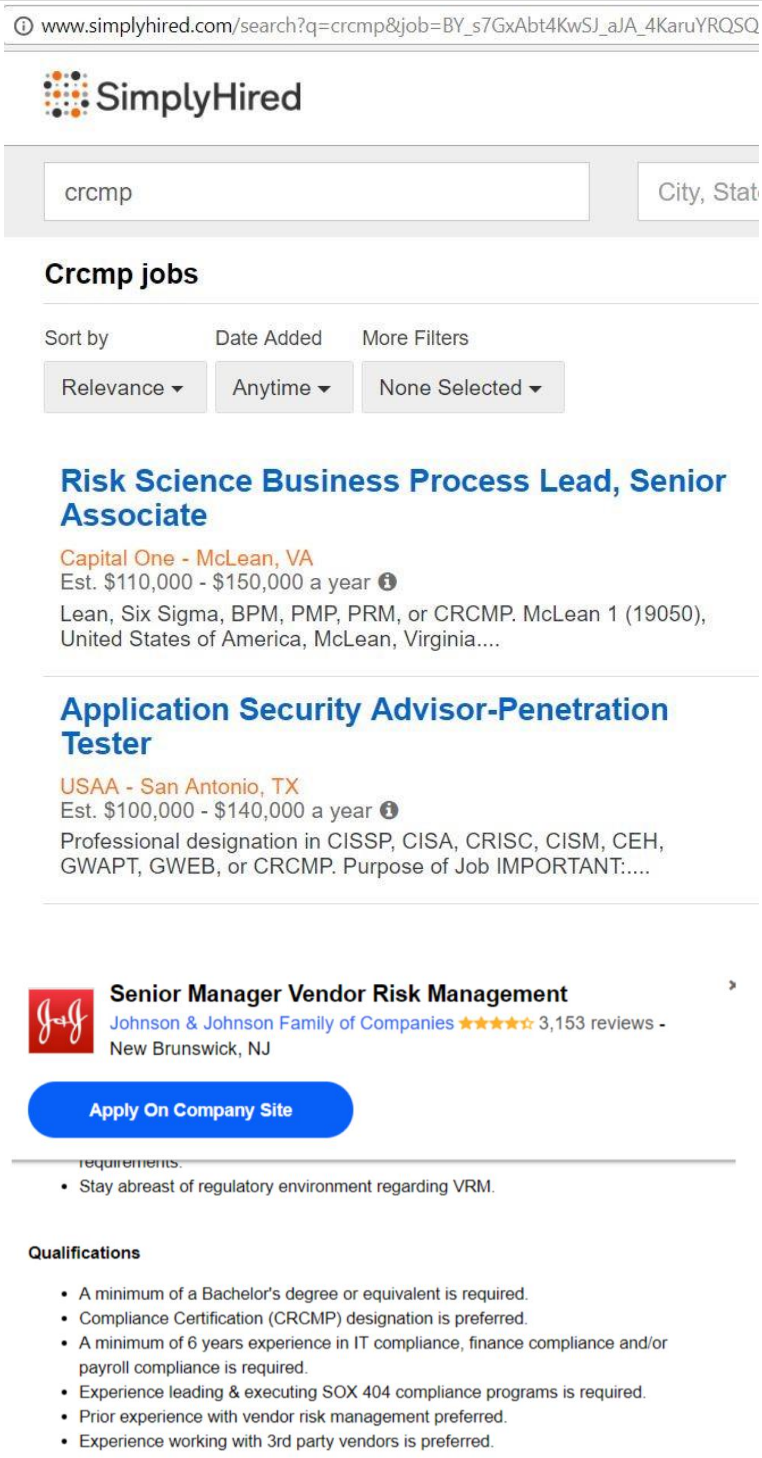
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- 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.