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, February 7, 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,

Once upon a time, *engineering* was the application of science to the optimum conversion of the resources of nature to the uses of humankind (source: Britannica).

The US Engineers Council for Professional Development has defined engineering as the creative application of scientific principles to design or develop structures, machines, apparatus, or manufacturing processes, or works utilizing them singly or in combination; or to construct or operate the same with full cognizance of their design; or to forecast their behaviour under specific operating conditions; all as respects an intended function, economics of operation and safety to life and property.

I have just read a paper from the European Network and Information Security Agency (ENISA) with title *"Data Protection Engineering"*. According to the paper, the data protection *by design* concept emerged several years ago in the context of *privacy engineering*.

Data Protection Engineering can be perceived as part of data protection *by Design* and *by Default*. It aims to support the selection, deployment and configuration of appropriate technical and organizational measures in order to satisfy specific data protection principles.

Undeniably it depends on the measure, the context and the application and eventually it contributes to the protection of data subjects' rights and freedoms.

In the paper, we can find some new compliance terminology and requirements:

"With regards to specific tools and technologies, another categorization can be based on the characteristics of the technology used in relation to the data being processed. More specifically, these characteristics can be:

• *Truth-preserving:* The objective of privacy engineering is to preserve the accuracy of data while reducing their identification power.

This goal can be achieved for instance diluting the granularity of data (e.g. from date of birth to age).

In this way data are still accurate but in a "minimized way", adequate for the purpose at stake.

Also, encryption may be regarded as a truth preserving technique, since encryption applied in the reverse direction fully restores the original data without injecting any uncertainty in the process.

• *Intelligibility-preserving:* Data are kept in a format which "has a meaning" for the controller, without disclosing real data subjects' attributes.

For instance, the trick of introducing an offset to a hospitalization date keeps the day/month/year format but breaks the link with the true data of an identified patient.

Also, the injection of noise is an intelligibility preserving techniques since it does not alter the look-and-feel of data providing confidentiality safeguard on the true data.

• *Operable Technology:* Mathematic and logic operations (e.g. a sum or a comparison) can be executed on the results of their applications. Operability does not necessarily entail intelligibility, since (as it will be said

in this report) there are families of encryption techniques in which the (non-intelligible) results are directly operable using operations that are correctly executable in the encrypted domain."

There are some difficult parts too: "From the *data protection engineering* perspective, communication channels should go beyond the provision of security as their core functionality and incorporate additional privacy enhancing characteristics, such as who can have access to the content of the communication, including the providers, location and access to the encryption keys, location and type of the provider, user information disclosed etc. Towards this direction, two technologies are being discussed below, namely End-to-End encryption and proxy routing."

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

Best regards,

George Lekatis
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)

Federal Reserve Board invites public comment on proposed guidance to implement a framework for the supervision of certain insurance organizations overseen by the Board

Number 2 (Page 8)

Data Protection Engineering

Number 3 (Page 11)

Statement on Pay versus Performance

Chair Gary Gensler, U.S. Securities and Exchange Commission

Number 4 (Page 13)

On returning inflation back to target

Catherine L. Mann, External Member of the Monetary Policy Committee, Bank of England

Number 5 (Page 16)

Cybersecurity at US federal agencies

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

Number 6 (Page 19)

Connecting the digital islands - next steps in trade finance

Eddie Yue, Chief Executive of the Hong Kong Monetary Authority, at the roundtable on "The Future of Trade Finance: Opportunities for Hong Kong, Asia and the World"

Number 7 (Page 23)

Recent Cyber Events: Considerations for Military and National Security Decision Makers

CCDCOE
NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE

Number 8 (Page 27)

DARPA Researchers Use Light on Chip to Drive Next-Generation RF Platforms

Integrated optical approaches could allow tuning over multiple frequency bands

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 9 (Page 29)

Neil Esho appointed Secretary General of the Basel Committee on Banking Supervision

Number 10 (Page 31)

NIST Updates FIPS 201 Personal Identity Credential Standard

The standard now goes beyond physical ID cards to include electronic tokens and one-time passwords.

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

Number 1

Federal Reserve Board invites public comment on proposed guidance to implement a framework for the supervision of certain insurance organizations overseen by the Board

The Federal Reserve Board invited public comment on proposed guidance to implement a framework for the supervision of certain **insurance** organizations overseen by the Board.

The proposed supervisory framework—for depository institution holding companies significantly engaged in insurance activities—would apply guidance and allocate supervisory resources based on the risk of a firm.

It would also formalize a supervisory rating system for these companies and describe how examiners work with state insurance regulators.

The proposed guidance would apply to any depository institution holding company that is an insurance underwriting company or that has over 25 percent of its consolidated assets held by insurance underwriting subsidiaries.

Comments will be accepted for 60 days after publication in the Federal Register.

Summary

The Board is seeking comment on a new supervisory framework for depository institution holding companies significantly engaged in insurance activities, or supervised insurance organizations.

The proposed framework would provide a supervisory approach that is designed specifically to reflect the differences between banking and insurance.

Within the framework, the application of supervisory guidance and the assignment of supervisory resources would be based explicitly on a supervised insurance organization's complexity and individual risk profile.

The proposed framework would formalize the ratings applicable to these firms with rating definitions that reflect specific supervisory requirements and expectations.

It would also emphasize the Board's policy to rely to the fullest extent possible on work done by other relevant supervisors, describing, in particular, the way it will rely more fully on reports and other supervisory information provided by state insurance regulators to minimize the burden associated with supervisory duplication.

To read more:
https://www.federalreserve.gov/newsevents/pressreleases/bcreg20220128a.htm

https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20220128a2.pdf

Number 2

Data Protection Engineering

The evolution of technology has brought forward new techniques to share, process and store data. This has generated new models of data (including personal data) processing, but also introduced new threats and challenges.

Some of the evolving privacy and data protection challenges associated with emerging technologies and applications include: lack of control and transparency, possible reusability of data, data inference and re-identification, profiling and automated decision making.

The implementation of the GDPR data protection principles in such contexts is challenging as they cannot be implemented in the traditional, "intuitive" way.

Processing operations must be rethought, sometimes radically (similar to how radical the threats are), possibly with the definition of new actors and responsibilities, and with a prominent role for technology as an element of guarantee.

Safeguards must be integrated into the processing with technical and organisational measures.

From the technical side, the challenge is to translate these principles into tangible requirements and specifications by requirements by selecting, implementing and configuring appropriate technical and organizational measures and techniques.

Data Protection Engineering can be perceived as part of data protection by Design and by Default. It aims to support the selection, deployment and configuration of appropriate technical and organizational measures in order to satisfy specific data protection principles.

Undeniably it depends on the measure, the context and the application and eventually it contributes to the protection of data subjects' rights and freedoms.

The current report took a broader look into data protection engineering with a view to support practitioners and organizations with practical

implementation of technical aspects of data protection by design and by default.

Towards this direction this report presents existing (security) technologies and techniques and discusses possible strengths and applicability in relation to meeting data protection principles as set out in Article 5 GDPR.

Based on the analysis provided in the report, the following conclusions and recommendations for relevant stakeholders are provided below:

1. Regulators (e.g. Data Protection Authorities and the European Data Protection Board) should discuss and promote good practices across the EU in relation to state-of-the-art solutions of relevant technologies and techniques. EU Institutions could promote such good practices by relevant publicly available documents.

2. The research community should continue exploring the deployment of (security) techniques and technologies that can support the practical implementation of data protection principles, with the support of the EU institutions in terms of policy guidance and research funding.

3. Regulators (e.g. Data Protection Authorities and the European Data Protection Board) and the European Commission should promote the establishment of relevant certification schemes, under Article 42 GDPR, to ensure proper engineering of data protection.

To read more:
https://www.enisa.europa.eu/publications/data-protection-engineering

Number 3

Statement on Pay versus Performance

Chair Gary Gensler, U.S. Securities and Exchange Commission

The Commission is reopening the comment period for a proposed rule for corporate disclosure of "pay versus performance." I support this proposed rule because, if adopted, it would strengthen the transparency and quality of executive compensation disclosure.

The rule proposal would fulfill a mandate from Congress under the Dodd-Frank Act of 2010, passed after the 2008 financial crisis.

"Pay versus performance" disclosures describe the relationship between the executive compensation an issuer actually paid and the financial performance of that issuer. Such disclosures would make it easier for shareholders to assess the company's decision-making with respect to its executive compensation policies.

The Commission has long recognized the value of information on executive compensation to investors. The first requirements to make disclosures about executive compensation originated in the 1933 Act. Since then, from time to time the Commission has continued to update compensation disclosure requirements.

In 2015, the Commission proposed rules to implement the Dodd-Frank Act's "pay versus performance" requirement. These proposed rules relied upon total shareholder return as the sole measure of financial performance. Some commenters expressed concerns that total shareholder return would provide an incomplete picture of performance.

In this reopening release, we are considering whether additional performance metrics would better reflect Congress's intention in the Dodd-Frank Act and would provide shareholders with information they need to evaluate a company's executive compensation policies.

I'm pleased to support today's reopening release and look forward to the public's feedback. I'd like to extend my gratitude to the members of the SEC staff who worked on this item, including:

- Renee Jones, Erik Gerding, Connor Raso, Lindsay McCord, Jennifer Zepralka, Anne Krauskopf, Angie Kim, and Jeb Byrne in the Division of Corporation Finance;

- Bryant Morris, Dorothy McCuaig, and Ken Alcé in the Office of the General Counsel;

- Jessica Wachter, Vlad Ivanov, Tara Bhandari, Mike Willis, Julie Marlowe, PJ Hamidi, Robert Miller, and Lauren Moore in the Division of Economic and Risk Analysis;

- Brian Johnson, Amanda Wagner, and Amy Miller in the Division of Investment Management; and

- Kristin Pauley, Marc Johnson, and Laura Metcalfe in the Division of Enforcement;

- Jonathan Wiggins, Omid Harraf, Larry Yusuf, and Mark Jacoby in the Office of Chief Accountant.

Number 4

On returning inflation back to target

Catherine L. Mann, External Member of the Monetary Policy Committee, Bank of England

Introduction and summary

As an international economist, I have always studied domestic economic conditions through the lens of global influences.

This year the UK offers an excellent laboratory. Global factors have been at the forefront of the inflation surge in the UK, and their effects will persist into early 2022. However, expectations for wages and prices for this year, if realized, could keep UK inflation strong for longer, which might then generate a reinforcing cost-price dynamic.

To return inflation to target, the Monetary Policy Committee's first line of defence is to dampen expectations of future price increases. Achieving an inflection in these expectations along with tailwinds from global factors could mean that a shallower path of future rate rises is needed to bring inflation back to target.

In the last half of 2021, UK CPI inflation surged, more than doubling from 2% in July to 5.4% in December.

Previously, average earnings had rebounded strongly from their trough in 2020 leading to headline wage inflation rates as high as 9% in the summer.

While some of these increases are due to base and compositional effects, demand and supply imbalances both in goods and labour markets built very quickly over the second half of the year.

Residual strength in both wages and prices likely will continue for a time into 2022 as the domestic and global mismatch of supply and demand slowly resolve, as firms try to recover margins eroded in 2021, and as labour markets stay tight.

Indeed, firms in the latest DMP panel (from December) expect to raise their prices by 5% in 2022 – a bit more than the 4% in 2021.

Meanwhile, firms expect continued upward pressure on pay growth in 2022 on the top of the 2-3.5% increases of 2021.

These expectations for prices and wages, if realized, are ingredients for headline inflationary pressures that could stay strong for longer, well into 2023. The question for monetary policy then becomes whether the real factors on the one hand and expectations on the other could together create a reinforcing cost-price dynamic.

Certainly, there are headwinds facing these price and wage expectations. Most importantly, will domestic and global demand in 2022 be strong enough for firms to pass through wage and cost increases into their prices? In the end, it is the collective outturns of business pricing that translates into inflation.

Monetary policy has a role to play in managing expectations as well as ensuring that the economic and financial conditions facing firms and workers are consistent with the 2% target.

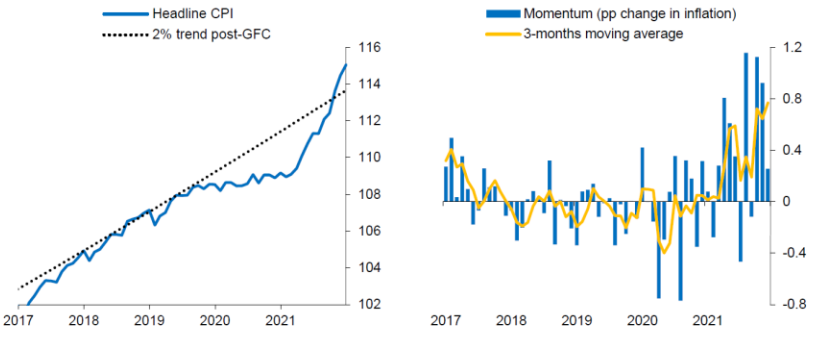
Initial conditions and the 2021 surge

Before we can assess the prospects for returning inflation to the 2% target, we need to recall initial conditions and review sources of the 2021 inflation surge.

Going into the pandemic, the UK CPI price level was roughly trending along its 2% inflation path, unlike in the US or the euro area which had seen persistently lower inflation than intended.

In the first year of the pandemic with lockdowns disrupting a wide range of activities, some firms did cut prices in the UK (and some markets simply did not exist, so there were no prices at all) and the aggregate price level flat-lined.

Chart 1: CPI level (index, LHS) and momentum (percentage points, RHS)

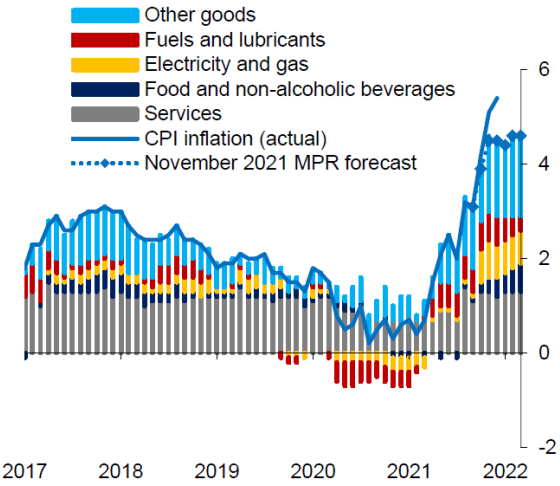


Sources: ONS and Bank calculations. Notes: Trend on LHS shows the level of prices if CPI had grown at 2% annualised rates in every month since December 2010. RHS shows momentum of CPI, i.e. the month-to-month percentage point change of year-on-year inflation. Thus, positive momentum means rising inflation (accelerating prices) and negative momentum falling inflation (decelerating prices). Latest observation: December 2021.

Both demand recovery and supply limitations in 2021 have now yielded robust inflation momentum, which if price expectations are realized, is poised to continue into 2022 moving the price level further away from the 2% trend. (Chart 1).

Reviewing key sources of the 2021 inflation surge – energy and core goods – both are importantly driven by sources external to the UK economy. (Chart 2).

Chart 2: Decomposition of CPI inflation in the November 2021 MPR forecast (% year-on-year)



Source: November 2021 Monetary Policy Report. Latest observation: December 2021 (actual), March 2022 (forecast).

Global goods prices have been elevated by the rotation away from consumer-facing services towards goods purchases.

The dominant driver of global goods price dynamics is the interplay of three successive US fiscal stimuli combined with geographical mismatches of containers and production stoppages in key economies and for key materials. But, a domestic equivalent to the global supply-demand imbalance has also been apparent in the UK, with production constraints and shortages of HGV drivers.

To read more:
https://www.bankofengland.co.uk/speech/2022/january/catherine-l-mann-speech-on-the-economy-and-monetary-policy-at-omfif

Number 5

Cybersecurity at US federal agencies

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

According to Shalanda Young, the acting director for the Office of Management and Budget (OMB), agencies will be transitioning to a "zero trust" approach that assumes no actor, system or network operating outside the security perimeter is to be trusted.

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

This memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. Those campaigns target Federal technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in Government.

I. OVERVIEW

Every day, the Federal Government executes unique and deeply challenging missions: agencies [1] safeguard our nation's critical infrastructure, conduct scientific research, engage in diplomacy, and provide benefits and services for the American people, among many other public functions. To deliver on these missions effectively, our nation must make intelligent and vigorous use of modern technology and security practices, while avoiding disruption by malicious cyber campaigns.

Successfully modernizing the Federal Government's approach to security requires a Government-wide endeavor. In May of 2021, the President issued Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*,[2] initiating a sweeping Government-wide effort to ensure that baseline security practices are in place, to migrate the Federal Government to a zero trust architecture, and to realize the security benefits of cloud-based infrastructure while mitigating associated risks.

This memorandum requires agencies to achieve specific zero trust security goals by the **end of Fiscal Year (FY) 2024**. These goals are organized using the zero trust maturity model developed by CISA. CISA's zero trust model describes five complementary areas of effort (pillars) (Identity, Devices, Networks, Applications and Workloads, and Data), with three

themes that cut across these areas (Visibility and Analytics, Automation and Orchestration, and Governance).

The strategic goals set forth in this memorandum align with CISA's five pillars:

1. Identity: Agency staff use enterprise-managed identities to access the applications they use in their work. Phishing-resistant MFA protects those personnel from sophisticated online attacks.

2. Devices: The Federal Government has a complete inventory of every device it operates and authorizes for Government use, and can prevent, detect, and respond to incidents on those devices.

3. Networks: Agencies encrypt all DNS requests and HTTP traffic within their environment, and begin executing a plan to break down their perimeters into isolated environments.

4. Applications and Workloads: Agencies treat all applications as internet-connected, routinely subject their applications to rigorous empirical testing, and welcome external vulnerability reports.

5. Data: Agencies are on a clear, shared path to deploy protections that make use of thorough data categorization. Agencies are taking advantage of cloud security services to monitor access to their sensitive data, and have implemented enterprise-wide logging and information sharing.

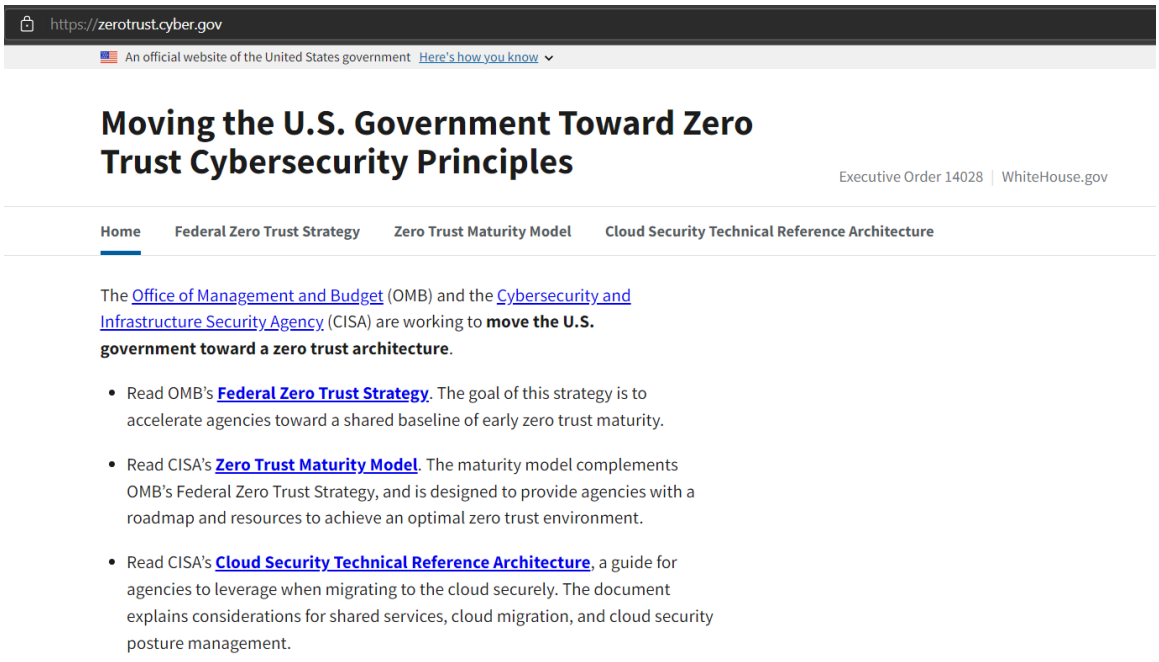
EO 14028 required agencies to develop their own plans for implementing zero trust architecture. Within 60 days of the date of this memorandum, agencies must build upon those plans by incorporating the additional requirements identified in this document and submitting to OMB and CISA an implementation plan for FY22-FY24 for OMB concurrence, and a budget estimate for FY24.

Agencies should internally source funding in FY22 and FY23 to achieve priority goals, or seek funding from alternative sources, such as working capital funds or the Technology Modernization Fund.

Agencies will have 30 days from the publication of this memorandum to designate and identify a **zero trust strategy implementation lead** for their organization.

OMB will rely on these designated leads for Government-wide coordination and for engagement on planning and implementation efforts within each organization.

OMB and CISA will work with agencies throughout zero trust implementations to capture best practices, lessons learned, and additional agency guidance on a jointly maintained website at https://zerotrust.cyber.gov/



To read more:
https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

Number 6

Connecting the digital islands - next steps in trade finance

Eddie Yue, Chief Executive of the Hong Kong Monetary Authority, at the roundtable on "The Future of Trade Finance: Opportunities for Hong Kong, Asia and the World", co-organised by the University of Hong Kong (HKU) Asia Global Institute & International Chamber of Commerce, Hong Kong

Good afternoon everyone. Thank you, Dr Fung, for inviting me to speak, and the HKMA is very pleased to support today's event. It would have been a pleasure to meet you all in person, but I am thankful that this event could go ahead as planned.

Today's topic is the future of trade finance, and I believe we all agree that, to elevate global trade finance to the next level, the recurring pain points of the existing trade finance system need to be fixed.

The issues-including a paper-based system that is inefficient, prone to fraud and human error-have been discussed many times; so I believe by now, we all have a basic understanding of the problems. Indeed, various stakeholders, including the HKMA, have been attempting to solve the pain points by using emerging technologies.

For example, in 2018, the HKMA facilitated the launch of eTradeConnect, which is a blockchain-based platform that aims to digitise paper-based documents and automate the trade finance process. The platform was subsequently connected to a similar platform built by the People's Bank of China to facilitate cross-boundary trade finance processes.

Similar platforms have proliferated around the world, but the trade finance gulf continues to widen. According to the Asian Development Bank, about 10% of global trade suffer from the trade financing gap.

To put this into perspective, the value of the gap amounted to USD $1.7 trillion in 2020, marking a 15% increase from just two years before. SMEs, in particular, accounted for an alarming 40% of rejected trade finance requests. These figures illustrated that global efforts are nowhere near enough, and we should all rethink why the gap is continuing to widen, and how to make our efforts as effective as possible.

A recent report published with the support of Fung Business Intelligence suggested a possible reason: the various digital trade finance platforms mostly work independently and do not synergise with each other, resulting in what we call digital islands.

It is as if we are all putting our heads down and concentrating on developing our own platforms, forgetting that it is equally important for the platforms to communicate and work with each other. As suggested in the report, interoperation between the platforms could help to further modernise the global trade finance ecosystem and close the gap.

The Commercial Data Interchange, also known as CDI, which the HKMA is building, is precisely designed with enhancing interoperability in mind. By way of introduction, CDI aims to enhance the sharing of commercial data. Currently, every time a bank wants to connect to a data provider, it has to set up a new, separate connection.

With CDI, each bank and data provider will only need a single connection to the CDI platform, allowing banks to quickly access the business data of corporates. Banks will also be able to conveniently and swiftly set up connections with new data providers because CDI uses standardised APIs and data models, and adopts existing mainstream industry standards such as the Legal Entity Identifier.

I mentioned that CDI is designed with improving interoperability in mind. Because the platform can link up scattered digital islands and smoothen data sharing, it has great potential to enhance trade financing process and improve SMEs' access to financing. Let me show you how this could be achieved with the aid of a story.

Mr Chu runs a small business called Chu Kee with the help of his wife and parents. Chu Kee imports chilled chicken from Guangdong and sells them to supermarkets all around Hong Kong. The delicious taste of the chilled chicken and the Chus' impeccable service quickly earned Chu Kee a big group of loyal customers.

A few years ago, when Mr Chu was trying to apply for loans from banks to expand the business, he was unable to produce the financial statements required because he had never properly prepared one before. The loan approval process ended up taking almost six months, and the experience left Mr Chu rather upset, unfortunately.

Last year, Mr Chu was ready to further expand Chu Kee, and decided to give CDI a try. This time, the banks, instead of asking for financial statements, obtained alternative data from various data providers through CDI. For

instance, from integrated online shopping platforms, banks learnt the amount of chilled chicken Chu Kee supplied to different supermarkets, and their value.

With the data, the banks understood Chu Kee's latest operating conditions better and made credit decisions speedily. Needless to say, before the data was used and shared, prior consent from Chu Kee was obtained. In the end, Mr Chu secured a substantial loan at a competitive interest rate, and was very pleased with the hassle-free experience.

Now, what if I tell you that the above is based on a true story? Yes, during the technical exploration stage, CDI has already, in real life, helped SMEs in Hong Kong take more control of their own digital footprint, and use their own data to improve their access to financial services.

Importers of chilled food and sneakers, and manufacturers of phone accessories have already enjoyed the benefits of CDI firsthand. As more and more banks and data providers join CDI, we expect that an increasing number of SMEs will benefit from the platform.

For CDI to reach its full potential and successfully connect the digital islands, your active participation is crucial. CDI is definitely a team sport, and we all have a role to play as members of Team Hong Kong.

The HKMA, as a regulator, will facilitate a conducive environment, and we are doing that by building the infrastructure and offering guidance. To banks, we urge you to embrace fintech, and join the CDI platform. To data providers, we invite you to contribute meaningful data, such as logistics data and procurement data between buyers and suppliers, to enrich the types of data available. To SME owners, we encourage you to contact your bank and understand more about CDI. Together, we can take Hong Kong's data ecosystem to new heights, and ultimately contribute to bridging the global trade financing gap.

The benefits of a more digitally integrated trade finance system are plentiful, that much is certain; and the HKMA strives to help bring about an enhanced system in collaboration with different stakeholders. We look forward to working with the International Chamber of Commerce (ICC) and the Fung Group in this regard so that the needs of the underserved segments can be better catered for.

Before I close, I'd like to take this opportunity to offer you a glimpse of the HKMA's vision of digitalising cross-border trade. For those of you who have been following our CBDC developments closely, you will know that we are working on a project called mBridge.

We have already developed a trial CBDC platform, and it has proven ability to speed up cross-border payments from multiple days to near real-time.

We are now exploring the feasibility of connecting eTradeConnect, CDI, and mBridge to strengthen the synergy between the three and further digitalise the cross-border trade process.

First, eTradeConnect will provide the infrastructure for digitalising trade finance, as well as support cross-boundary trade between Hong Kong and Mainland China.

Second, CDI will link up various digital islands to form a seamless data ecosystem. And finally, mBridge will expedite cross-border payments while reducing costs.

We believe that the combined power of the three infrastructure would pave the way for digitalising cross-border trade in the trade corridor between Hong Kong, Mainland China, and other APAC regions. I hope to share further updates with you in the not-so-distant future, and in the meantime, I welcome your feedback and suggestions.

Thank you, and an early Happy Chinese New Year to you all. Wishing you all health, happiness, and good fortune in the Year of the Tiger.

Number 7

Recent Cyber Events: Considerations for Military and National Security Decision Makers

Reflections on 2021

2021 was an exciting year from a cybersecurity and cyber defence perspective. After dealing with the Solarwinds breach at the beginning of the year, the world experienced a series of serious ransomware incidents, in some cases causing disturbances to essential services.

We also saw governments expressing their commitment to protecting critical services and to responding forcefully to nations carrying out malicious cyber operations or allowing criminals to do so.

While impossible to cover all these developments in a brief report, we will take this opportunity to reflect on three important topics: ransomware, software supply chain security and spyware.

Perhaps looking at these from a little distance will help us see the larger picture and allow us to prepare better for the future.

The ransomware threat

Malicious cyber activity has grown substantially over the past two years while the world has been learning how to keep turning with the omnipresent pandemic.

One particular malware category, ransomware, made headlines frequently in 2021, partly because the operations were increasingly targeting high-value targets.

One of the first major ransomware incidents in 2021 may have been against the automakers Kia and Hyundai, although this has been denied by the alleged victims.

The actors behind the compromise appear to have used the now common double extortion tactics, not only causing an outage but also threatening to expose data exfiltrated from the victims' systems.

In March, CNA Financial, the seventh-largest commercial insurer in the US, fell victim to ransomware.

Shortly thereafter in April, the North American division of Brenntag, a German chemical distributor, faced a ransomware infection of their systems as well.

One of the most public ransomware incidents of this year was against Colonial Pipeline in May, an incident that was discussed in a previous issue of this series.

The largest fuel pipeline was shut down as a result of a ransomware attack. This led to fuel shortages across the US East Coast and an increase in fuel prices.

In the same month JBS, one of the largest meat suppliers in the US, suffered a compromise which caused it to temporarily shut down five of its plants and this also affected operations in the UK and Australia.

In July, Kaseya, an international IT service provider, announced it had fallen victim to ransomware which affected and shut down numerous companies in several countries.

For example, Sweden's third largest grocery chain had to close down 800 stores for several days, some of them in remote areas with very few to no alternatives.

Over the past two years, hospitals have also seen an increase in malicious cyber operations, though not limited to ransomware.

One of the most prominent victims was Ireland's health service which resulted in stolen patient data, the cancellation of appointments and delayed treatment.

Other known incidents targeted health companies in the US and New Zealand.

These attacks not only show how closely linked our society and systems have become, but also how vulnerable and highly dependent on the functioning of national critical infrastructure (CI) our societies now are.

According to the Department of Homeland Security (DHS), 16 CI sectors are considered to be of vital importance for the population of the US.

Similar examples of sectorial divisions of CI can be found in almost any country; for example, 12 have been identified in France and 13 in the UK.

The incidents mentioned above have all affected one or more of those sectors.

Due to the close interconnection of systems and services, all sectors are potential targets and a compromise of one can have a domino effect on others with severe consequences.

It is therefore of the utmost importance that nations define and strengthen their CI sectors and put in place contingencies to deal with any compromise.

Resilience need not only be built by having more robust or redundant digital systems. In many instances, we need to be prepared to operate without industrial control systems, or even to compensate for services affected by a cyberattack by other means, such as using local electrical generators to compensate for a power outage or to ship oil by sea or rail if pipelines are not operational.

Most of the companies targeted in the examples ended up paying ransom up to as high as $40 Million, even though the FBI and others advise against paying a ransom as it is no guarantee of getting data back and it incentivises criminals.

Discussions of public response to cyber threats have entered the military and political level as never before, with many states beginning to take steps both towards increasing the cyber security of CI on a national level through regulations or imposing costs on those responsible for malicious cyber operations.

This is intended to constitute deterrence both by denial of benefits and by the threat of retaliation.

The US government, for example, has taken a more active stance and combined resources from Cyber Command, NSA and other agencies and from international partners to lift responsibility to an all-of-government effort, including law enforcement.

Public declarations will need to be followed by clear action such as the reported capture of 12 suspects for involvement in ransomware operations by Europol in November 2021.

This type of layered approach to deterrence is critical to any kind of success and we can only hope that this will continue in the new year and that the results of such an approach will soon grow.

To read more:
https://ccdcoe.org/uploads/2022/02/Report_Reflections_on_2021_A4.pdf

Number 8

DARPA Researchers Use Light on Chip to Drive Next-Generation RF Platforms

Integrated optical approaches could allow tuning over multiple frequency bands

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Radio frequency (RF) and microwave signals invisibly permeate the environment around us, carrying everything from radar signatures to the data from our mobile phones.

Within RF systems, electronic oscillators can act as precise clocks or directly generate the baseline microwave tones.

While an ideal oscillator provides a tone at a singular frequency, component imperfections and coupling to the environment introduce significant phase noise to real-world sources.

Military and commercial drivers for better oscillators are plentiful: Close-to-carrier phase noise is a primary factor preventing the detection of small or slow-moving targets in Doppler radar, while in RF communications, timing jitter dictates the sampling precision of receivers and limits signaling bandwidth.

In the last decade, major advances in RF oscillator performance have been realized using optical techniques to synthesize high-fidelity microwave signals (i.e., frequencies from 1 to 100 GHz). Such RF oscillators typically employ optical frequency division (OFD) to achieve low phase noise that can reach record-setting levels.

Current solutions sacrifice other important attributes, however, in pursuit of spectral purity. Such trade-offs are problematic because module size, cost, tunability, and environmental sensitivity are also critical factors that determine the applicability of microwave sources to commercial and military systems.

The Generating RF with Photonic Oscillators for Low Noise (GRYPHON) program seeks to defy today's tradeoffs by leveraging recent advancements in the miniaturization, integration, and volume production of precision optical components through lithographic microelectronic fabrication.

"Nonlinear integrated photonics provides a path to achieve incredible oscillator performance while reducing system size by orders of magnitude," says Dr. Gordon Keeler, program manager in DARPA's Microsystem

Technologies Office. “Beyond the cost and size advantages, integrated optical approaches could allow tuning over multiple frequency bands and environmental robustness. There is potential for very broad impact if our teams are successful.”

The first technical area the GRYPHON program will pursue is to develop low noise, compact, and frequency-agile prototypes that can provide outputs spanning 1-40 GHz.

The prototype target performance metrics are geared toward rapid adoption by military and commercial entities alike. Program success will also hinge on proving robustness to environmental effects and demonstrating a roadmap to high-volume, low-cost domestic manufacturing.

The research teams selected for this endeavor include: Honeywell, Nexus Photonics, BAE Systems, Caltech, and hQphotonics. Due to the highly interdisciplinary nature of the work, most performers have engaged additional partners to complement their core competencies.

GRYPHON’s second technical area encourages performers to pursue advanced techniques that offer even lower phase noise or ultra-wide tunability to inform future oscillator architectures. Teams from Columbia University and University of Virginia have been selected to push the boundaries in materials and system integration to this end.

With a diversity of approaches, materials, and performer teams, the GRYPHON program promises to deliver high impact solutions in the near term and germinate future directions for exploration.

Number 9

Neil Esho appointed Secretary General of the Basel Committee on Banking Supervision

- Neil Esho appointed Secretary General of the international standard-setter

- His term starts in February 2022 for three years

- Mr Esho previously served as Deputy Secretary General of the Basel Committee

The Basel Committee on Banking Supervision today announced the appointment of Neil Esho as its next Secretary General for an initial term of three years. He succeeds Carolyn Rogers, who had served as Secretary General since 2019, and left the Committee in November to become Senior Deputy Governor of the Bank of Canada.

Mr Esho has been Deputy Secretary General since July 2014. He joined the Basel Committee Secretariat in April 2006. Prior to that, he was Head of Research at the Australian Prudential Regulation Authority (APRA).

Before joining APRA in 2001, he was a Senior Lecturer at the School of Banking and Finance at the University of New South Wales. He holds a PhD in finance from the University of New South Wales.

I am delighted to announce Neil's appointment as Secretary General. His extensive supervisory and regulatory background, and the instrumental role he has played in supporting the development of standards such as the Basel III framework, place him in an ideal position to lead the Secretariat in the next phase of the Committee's work as it focuses on implementation as well as on new challenges around cryptocurrencies, climate-related financial risks and the accelerating digitalisation of finance.

I would also like to once again thank Carolyn Rogers for her dynamic leadership, particularly her able steering of the Basel Committee through the Covid-19 pandemic and its many challenges. She has put it on a sound footing to face the changing international banking landscape.

Pablo Hernández de Cos, Chair of the Basel Committee and Governor of the Bank of Spain

Neil's deep understanding of the Basel Committee's work and the key role he has played in implementing its agenda over the past 15 years will be invaluable as he takes the lead of the Secretariat at this crucial time.

I would also like to express my appreciation for the efforts of his predecessor, Carolyn Rogers, for so strongly setting out the case for the full, consistent and timely implementation of the Basel III standards, and look forward to further progress with Neil's support.

François Villeroy de Galhau, Chairman of the Basel Committee's oversight body, the Group of Central Bank Governors and Heads of Supervision (GHOS), and Governor of the Bank of France

Number 10

NIST Updates FIPS 201 Personal Identity Credential Standard

The standard now goes beyond physical ID cards to include electronic tokens and one-time passwords.

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

To ensure that federal employees have a broader set of modern options for accessing facilities and electronic resources, the National Institute of Standards and Technology (NIST) has increased the number of acceptable types of credentials that federal agencies can permit as official digital identity.

The increase is part of the latest update to Federal Information Processing Standard (FIPS) 201, which specifies the credentials that can be used by federal employees and contractors to access federal sites.

The update, formally titled FIPS 201-3: Personal Identity Verification (PIV) of Federal Employees and Contractors, also allows for remote identity proofing and issuing, in addition to doing so in-person as was previously required.

“We have expanded the set of credentials that can be used for gaining access to federal facilities and also for logging onto workstations and other IT resources,” said Hildegard Ferraiolo, a NIST computer scientist. “It’s not all about PIV cards anymore.”

The preceding FIPS standard, version 201-2, came out in 2013 and specified credentials embedded on PIV cards as the primary means for authentication, with limited exceptions for credentials designed for mobile devices that lacked PIV card readers. Millions of PIV cards have been issued to federal employees.

The 201-3 update, the result of a regular review cycle, still specifies that PIV cards can be used but now offers additional options.

It keeps the standard aligned with the most recent federal policies, including the Office of Management and Budget’s Memorandum M-19-17 on identity, credential and access management.

It also ensures that the standard reflects current technological capabilities and needs, Ferraiolo said.

“It has become important to provide more flexibility to agencies in choosing credentials to use for authentication,” she said. “Not all laptop computers

are available with built-in PIV card slots, for example, and often, there are cloud-based applications that don't use public-key infrastructure that PIV cards provide. For these situations we need alternatives."

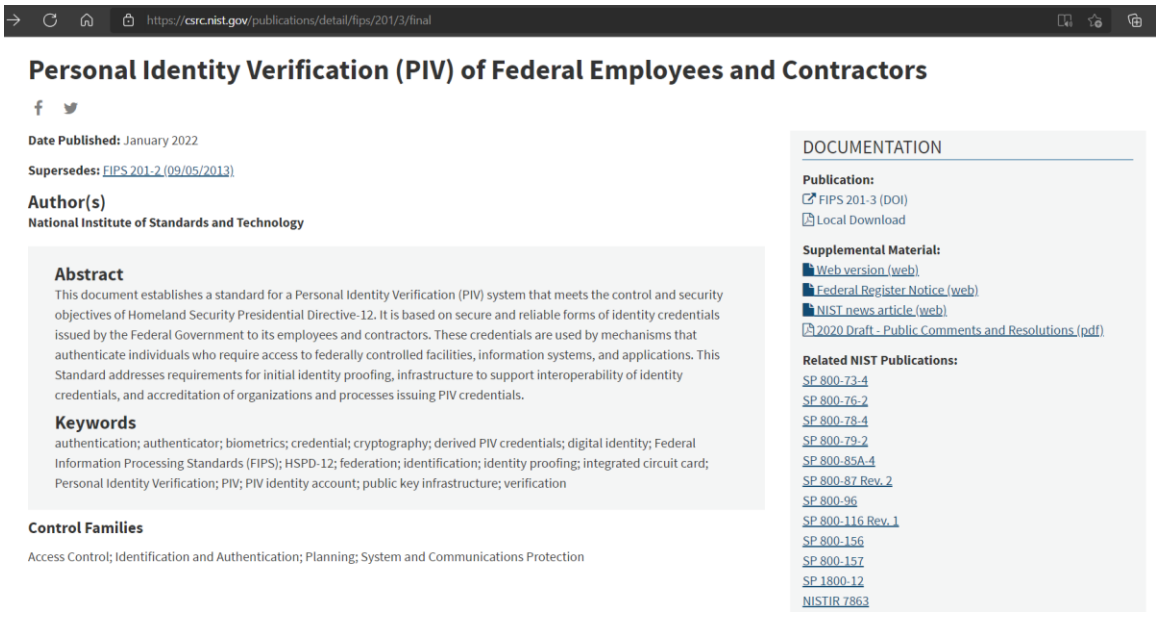
The new options are a subset of credentials that are specified in NIST SP 800-63-3, a multivolume publication on digital identity. Branches of the government will have a richer set of multifactor credentials for different devices — including, for example, FIDO (Fast ID Online) tokens and one-time passwords (OTP).

With the revision milestone now complete, the focus for NIST has shifted to providing additional guidelines and implementation details, Ferraiolo said. NIST is currently in the process of updating guidelines for the expanded set of PIV credentials in Revision 1 of NIST SP 800-157.

Additionally, to ensure that different credentials are interoperable across different agencies, a concept known as "federation," NIST will provide guidelines in NIST SP 800-217.

Ferraiolo said these and other NIST publications associated with FIPS 201-3 would be updated in coming months.

For more information, see the complete FIPS update, which is available online at: https://csrc.nist.gov/publications/detail/fips/201/3/final



FIPS PUB 201-3

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION
(Supersedes FIPS 201-2)

Personal Identity Verification (PIV) of Federal Employees and Contractors

CATEGORY: INFORMATION SECURITY **SUBCATEGORY: IDENTITY**

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.201-3

Issued January 2022

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.

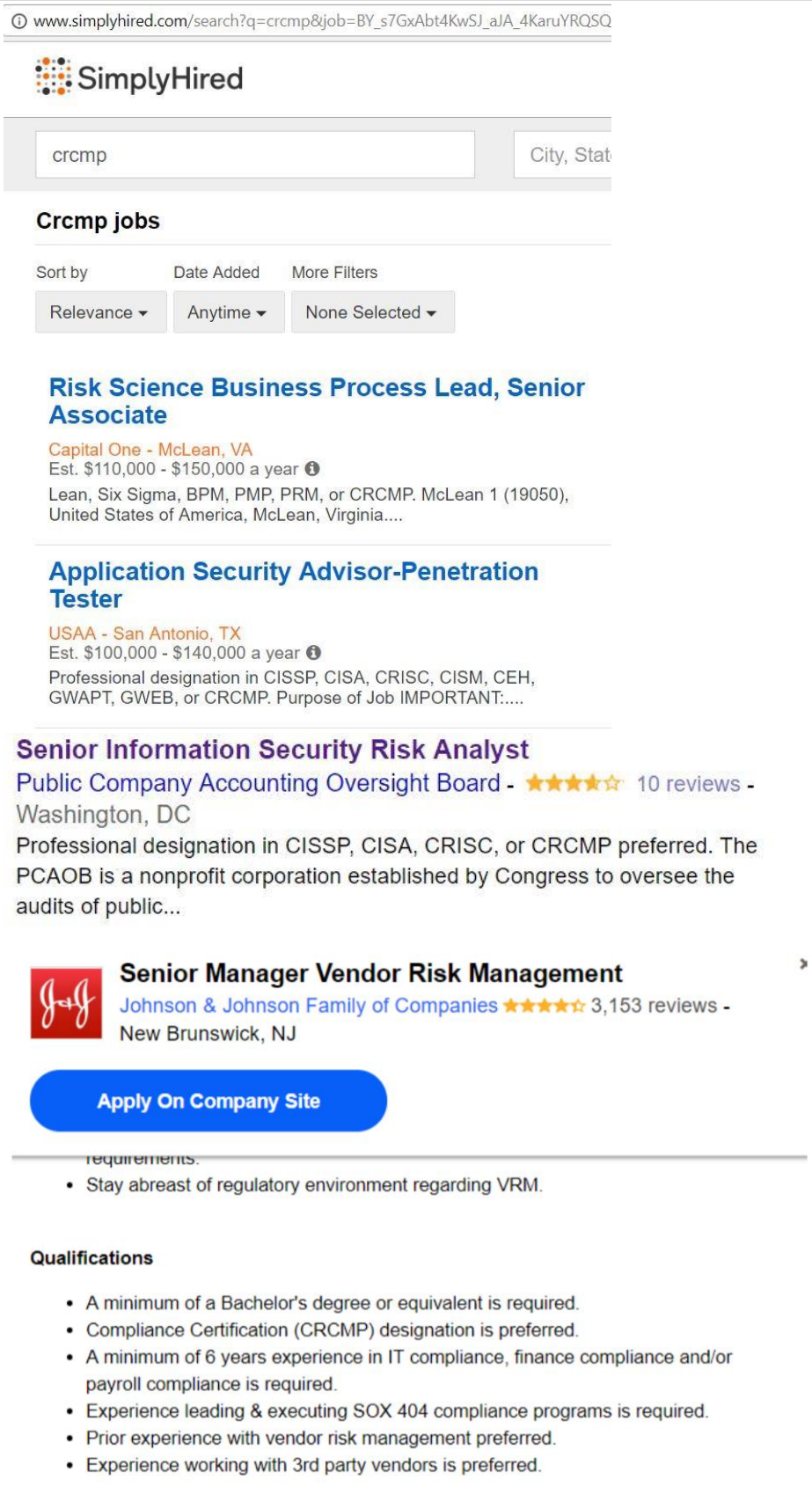
International Association of Risk and Compliance Professionals

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



Companies and organizations like Accenture, American Express, USAA etc. consider the Certified Risk and Compliance Management Professional

(CRCMP) program a preferred certificate. There are CRCMPs in 32 countries.

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

Our Reading Room:
https://www.risk-compliance-association.com/Reading_Room.htm