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, July 26, 2021

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,

Almost a year ago, we had an interesting paper from the FSB, with title *"Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements, Final Report and High-Level Recommendations"*.

According to the paper, the so-called "stablecoins" are a specific category of crypto-assets which have the potential to enhance the efficiency of the provision of financial services, but may also generate risks to financial stability, particularly if they are adopted at a significant scale.

While such financial stability risks are currently limited by the relatively small scale of these arrangements, this could change in the future.

Stablecoins are an attempt to address the high volatility of "traditional" crypto-assets by tying the stablecoin's value to one or more other assets, such as sovereign currencies. They have the potential to bring efficiencies to

payments (including cross-border payments), and to promote financial inclusion. However, a widely adopted stablecoin with a potential reach and use across multiple jurisdictions (so-called *"global stablecoins" or GSCs)* could become systemically important in and across one or many jurisdictions, including as a means of making payments.

These are the important "FSB High-Level recommendations to address the regulatory, supervisory and oversight challenges raised by GSCs arrangements".

1. Authorities should have and utilise the necessary powers and tools, and adequate resources, to comprehensively regulate, supervise and oversee a GSC arrangement and its associated functions and activities, and enforce relevant laws and regulations effectively.

2. Authorities should apply comprehensive regulatory, supervisory and oversight requirements and relevant international standards to GSC arrangements on a functional basis and proportionately to their risks.

3. Authorities should cooperate and coordinate with each other, both domestically and internationally, to foster efficient and effective communication and consultation in order to support each other in fulfilling their respective mandates and to ensure comprehensive regulation, supervision, and oversight of a GSC arrangement across borders and sectors.

4. Authorities should ensure that GSC arrangements have in place a comprehensive governance framework with a clear allocation of accountability for the functions and activities within the GSC arrangement.

5. Authorities should ensure that GSC arrangements have effective risk management frameworks in place especially with regard to reserve management, operational resilience, cyber security safeguards and AML/CFT measures, as well as 'fit and proper' requirements.

6. Authorities should ensure that GSC arrangements have in place robust systems for collecting, storing and safeguarding data.

7. Authorities should ensure that GSC arrangements have appropriate recovery and resolution plans.

8. Authorities should ensure that GSC arrangements provide users and relevant stakeholders with comprehensive and transparent information necessary to understand the functioning of the GSC arrangement, including with respect to its stabilisation mechanism.

9. Authorities should ensure that GSC arrangements provide legal clarity to users on the nature and enforceability of any redemption rights and the process for redemption, where applicable.

10. Authorities should ensure that GSC arrangements meet all applicable regulatory, supervisory and oversight requirements of a particular jurisdiction before commencing any operations in that jurisdiction, and adapt to new regulatory requirements as necessary.

Today we have an interesting paper with title *"Central bank digital currencies for cross-border payments, Report to the G20, July 2021"*. It uses the FSB definition of stablecoins, and it discusses examples like the "Sand Dollar" from the Central Bank of The Bahamas (CBoB).

The Sand Dollar is only for domestic use, non-domestic payees are excluded. Non-residents can transact and hold Sand Dollars when visiting the Bahamas by registering for the Tier 1 Sand Dollar wallet, with a holding limit of 500 Sand Dollars and a transaction limit of 1,500 Sand Dollars per month. The CBoB allows holders of a Sand Dollar account to integrate with traditional bank accounts, which can then be used to make cross-border payments using traditional channels.

You can read more at number 3 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 6 (Page 26)

A new strategy for a changing world

Isabel Schnabel, Member of the Executive Board of the European Central Bank, at a virtual event series, hosted by the Peterson Institute for International Economics.

Number 7 (Page 28)

China Requires Researchers to Report All Zero-Day Vulnerabilities

中共中央网络安全和信息化委员会办公室
Office of the Central Cyberspace Affairs Commission

Number 8 (Page 29)

Operation SpoofedScholars: report into Iranian APT activity

National Cyber Security Centre

Number 9 (Page 30)

Competition and collaboration: Understanding interacting epidemics can unlock better disease forecasts

A new algorithm increases scientists' abilities to accurately model mutually dependent spreading processes, from virus outbreaks to disinformation on social media, by Andrey Lokhov

Los Alamos NATIONAL LABORATORY

Number 10 (Page 31)

NIST Evaluates Face Recognition Software's Accuracy for Flight Boarding

Agency's new test concerns checking in passengers and documenting their exit from a country.

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

Number 1

Disclosures and Data: Building Strong Foundations for Addressing Climate-Related Financial Risks

Vice Chair for Supervision Randal K. Quarles, at the Venice International Conference on Climate Change, Venice, Italy

Introduction

Thank you for inviting me today. It is an honor to be here and, after more than a year of remote conversations, it is truly wonderful to see so many people in person.

As Chair of the Financial Stability Board (FSB), I have the privilege of collaborating with the Italian G20 Presidency, the G20 Finance Ministers and Central Bank Governors, and with the FSB membership on the most pressing issues affecting financial stability.

Among those issues, one of increasing focus is understanding and monitoring climate-related financial risks. Given the global nature of climate change, this demands a coordinated international effort.

The FSB published last Wednesday a Climate Roadmap that presents a comprehensive and coordinated plan to address climate-related financial risks. The FSB's roadmap dovetails with the ongoing work of the G20 Sustainable Finance Working Group (SFWG) to develop a broader sustainable finance roadmap.

Today, in my role as Chair of the FSB, I would like to focus on the two foundational components of the FSB roadmap: disclosures and data. Globally consistent, comparable, and reliable disclosures, as well as a broader set of high-quality, relevant data, together, can provide the basis to assess climate-related financial risks and the impact on financial stability.

Disclosure

The FSB was an early leader in bringing attention to the importance of reliable, entity-level disclosures to assess and manage climate-related financial risks and opportunities. In 2015, the FSB submitted a proposal to

the G20 to create an industry-led disclosure task force on climate-related risks.

The work of this FSB-sponsored Task Force on Climate-related Financial Disclosures, or TCFD, has led to greater recognition of the importance of climate-related financial risk and of comparable and reliable disclosure.

The early development of industry-led recommendations and a usable framework by users and producers of this information was critical.

The four core elements of the TCFD recommendations have provided a widely accepted framework for disclosures—covering governance, strategy, risk management, and metrics and targets.

The task force has continued to provide significant support to those seeking to disclose and has encouraged steadily increasing uptake.

These initial steps greatly helped to define appropriate parameters, drive towards consistency, and give the public sector a running start in developing their own approaches.

Now it is time to build on that work. It will be useful to establish a globally consistent baseline standard for climate-related disclosures.

Globally consistent and comparable entity-level disclosures by non-financial companies, banks, insurers, and asset managers are increasingly important to market participants and financial authorities as a means of providing information needed to assess and manage risks.

The G20 Presidency, in developing its 2021 work program, asked the FSB to encourage more consistency in disclosure practices.

As a start, the FSB surveyed what financial authorities across our membership were doing to promote disclosures. Almost all our members have already set requirements, guidance, or expectations or plan to do so.

We found some heterogeneity in the approaches they were taking. Some members prefer mandated disclosure while others would make it voluntary.

There is also variation in the desired scope of disclosures.

However, there is a trend towards an important baseline that focuses on one-way materiality—or the financial risk that climate change could have on a particular entity—based on the TCFD recommendations.

The majority of our membership are already using the TCFD recommendations as a baseline for their own requirements or guidance.

The International Financial Reporting Standards Foundation (IFRS), in consultation with other international organizations, will develop a set of standards, starting initially with climate and building upon these TCFD recommendations.

As reflected in our December 2020 statement, the FSB supports IFRS's advancement of an International Sustainability Standards Board to take this work quickly forward.

This work holds the promise of providing baseline standards that could inform or be built upon by national authorities as they develop their approaches to climate-related financial disclosure or broader sustainability disclosure.

The initial focus of the IFRS will be on climate standards, while allowing for interoperability with individual jurisdictions' frameworks, that may go beyond climate-related impacts.

Consistency in one-way disclosures would provide a needed avenue for accurate and appropriate risk assessment and comparability to assess investment decisions. Simultaneously, the IFRS standards are intended to provide flexibility for national authorities to build on the baseline.

The "interoperability" feature will allow jurisdictions to address broader or jurisdiction-specific concerns in a manner consistent with their legal and regulatory frameworks, and indeed to go further in scope or faster if they wish. Given the importance of this work, we encourage the IFRS to press forward as quickly as possible.

In the interim, the FSB continues to encourage jurisdictions that are implementing frameworks to base them on the TCFD recommendations to avoid unnecessary fragmentation.

Data

The need for high quality, reliable data doesn't stop at firms' disclosures, however. International initiatives are needed to improve data quality and address data gaps, and ultimately to establish a basis of comprehensive, consistent, and comparable data for global monitoring and assessing climate-related financial risks. We published a separate report on this topic last week.

Our data needs include data on the underlying drivers of physical and transition risk and financial institutions' exposures. The challenges here are considerable.

To understand the financial risks, better information is needed on the underlying physical risks, including the sorts of extreme weather events that pose greatest risks to the balance sheets of households, firms, and financial institutions.

Comparable data is also needed on the nature of jurisdictions' climate-change targets and progress in meeting them. All this information needs to be related to financial risks—including financial institutions' exposures to non-financial counterparties.

This is not an easy task. The current lack of usable data is a reflection of difficulties in transforming existing information on the drivers of climate risk into reliable metrics that quantify financial risks.

The key here is to find metrics that are forward-looking, recognizing that the nature and magnitude of future climate-related risks may differ from those in the past.

Improved financial risk data can also help achieve the financial stability mandates of financial authorities.

For example, the FSB is exploring how to assess the degree to which climate-related risks might be transferred or amplified by different financial sectors, including the interdependence of banks and insurance firms.

Climate-related risks vary across jurisdictions, and we need to look at how risks might be amplified by feedback loops with the real economy.

Such analysis will contribute to a more comprehensive and global understanding of how to assess climate change and potential effects on the financial system, but those efforts are hampered by a variety of data limitations.

The FSB is working with international bodies, such as the International Monetary Fund, and other international groupings, such as the Network for Greening the Financial System (NGFS), to assess climate data gaps and to identify steps to address them, with a special emphasis on ensuring cross-sectoral and international consistency.

For example, the FSB plans to coordinate work with the NGFS on the issues surrounding scenario analyses, which some jurisdictions are using or contemplating, and the financial metrics that would be useful for such an analysis, both at the level of the firm and the overall system.

Examining scenario analysis presents many challenges: A very long time horizon—which requires dynamic balance-sheet analysis—and the need to capture the interplay between the macro-economy and drivers of climate-related risks are two such challenges that would need to be overcome.

Conclusion

Today, the FSB is well-positioned to lead in the next phases of the work required to assess and address climate-related financial risk.

The FSB's mandate, its diverse membership, and its connection to the G20 make it the ideal forum to forge a consensus on the appropriate path forward.

The FSB, as laid out in its roadmap, has taken on a critical role in coordinating and carrying forward work that will make the global financial system more resilient to the threats posed by climate change.

The roadmap establishes a strategic vision for addressing climate-related financial risks, which sets out how we will coordinate with other standard-setting bodies and international organizations in order to progress towards our goal.

Our Climate Roadmap leverages the FSB's strength as a coordinating body, provides some structure to the vast amount of work on climate-related financial risks currently going on internationally, and clarifies interdependencies between workstreams and between issues.

The Climate Roadmap sets the course and promotes consistency through, among other things, building consensus around common principles, best practices, and cross-jurisdictional alignment.

These include the two broad objectives that I have focused on today—establishing consistent, comparable, and reliable information through a global baseline standard for disclosures and through improving the availability and quality of data.

The roadmap also includes work on analytical tools and policy approaches developed for identifying and managing climate-related financial risks.

We have a long road ahead of us, but every journey begins with the first steps. The FSB will continue to leverage its strengths to coordinate and contribute to understanding and addressing the challenges to the financial system that arise from these risks.

Number 2

Early lessons from the Covid-19 pandemic on the Basel reforms

BIS

Executive summary

Beginning in 2009, the Basel Committee on Banking Supervision (the Committee) developed a set of new regulatory standards, commonly referred to as the Basel reforms, in response to the Global Financial Crisis of 2007–09.

These standards aimed to strengthen the regulation, supervision and risk management of banks. Following their issuance, the Committee has deemed it appropriate to evaluate the impact of those standards already implemented on the resilience and behaviour of the banking system.

As part of this evaluation, the Committee has started to assess the ongoing Covid-19 pandemic's impact on the banking system, as it has posed a significant global test of the Basel reforms.

This report provides a preliminary assessment of whether the reforms implemented thus far have functioned as intended in light of the pandemic, which has resulted in a pronounced global economic shock, albeit one significantly different in nature from the financial crisis that motivated the Basel reforms.

The report reflects the Committee's initial findings based upon empirical analysis of a combination of vendor and regulatory data, case studies and the results of a supervisory survey conducted by the Committee.

The findings of this report should be considered in light of

(i) the incomplete data available to date regarding the impact of the pandemic, which continues to unfold and whose full effect on the economy may not yet be clear, and

(ii) the difficulty of distinguishing between the effects of the Basel reforms and those of the extensive and wide-ranging monetary and fiscal support measures undertaken by authorities to address the economic impact of the pandemic.

The report finds that the increased quality and higher levels of capital and liquidity held by banks have helped them absorb the sizeable impact of the Covid-19 pandemic thus far, suggesting that the Basel reforms have

achieved their broad objective of strengthening the resiliency of the banking system. Banks and the banking system would have faced greater stress had the Basel reforms not been adopted.

Throughout the unprecedented global economic downturn the banking system has continued to perform its fundamental functions, as banks have continued to provide credit and other critical services.

While the report finds that some features of the Basel reforms, including the functioning of capital and liquidity buffers, the degree of countercyclicality in the framework, and the treatment of central bank reserves in the leverage ratio may warrant further consideration, it does not seek to draw firm conclusions regarding the need for potential revisions to the reforms.

Following a brief narrative regarding the impact of the pandemic on the banking system (Section 1), this report outlines the Committee's initial findings regarding

(i) the overall resilience of the banking system during the pandemic (Section 2);

(ii) the usability of capital buffers, members' experience with the countercyclical capital policies and price movements of Additional Tier 1 (AT1) capital instruments (Section 3);

(iii) liquidity buffers (Section 4);

(iv) the impact of the leverage ratio on financial intermediation (Section 5); and

(v) the cyclicality of specific Basel capital requirements (Section 6).

The overall resilience of the banking system during the pandemic

As noted, the analysis indicates that the banking system has remained resilient through the pandemic, strengthened by substantial increases in capital and liquidity held by banks since the adoption of the Basel reforms.

No internationally active bank has failed or required significant public sector funding since the onset of the pandemic, though future losses may emerge as the pandemic remains ongoing.

Banks have generally managed to absorb temporary increases in the costs of liquidity and higher credit risk while substantially maintaining their

services to customers. Market measures of resilience (eg banks' credit default swap (CDS) spreads) do, however, indicate that some banks experienced strain early in the pandemic.

Regression results suggest that banks with higher Common Equity Tier 1 (CET1) capital ratios experienced smaller increases in CDS spreads.

Moreover, the analysis indicates that more strongly capitalised banks showed greater increases in lending to businesses and households than other banks.

Thus, the global banking system has been able to complement and support monetary and fiscal authorities' efforts to maintain economic activity during the pandemic, helping to absorb the shock rather than amplifying it, as occurred during the 2007–09 financial crisis.

The usability of capital buffers and price movements of AT1 capital instruments

The analysis indicates that most banks maintained capital ratios well above their minimum requirements and buffers during the pandemic partially due to authorities reducing capital requirements and buffers and imposing restrictions on capital distributions via dividend payments and share buybacks, as well as due to the extensive fiscal and monetary support provided to borrowers.

This makes it difficult to draw conclusions regarding banks' willingness to use capital buffers. Though some evidence suggests that banks may have been hesitant to use their regulatory capital buffers had it been necessary.

Regression results, including a detailed study of loan data from the euro area, indicate that banks that had less headroom (ie the amount of capital resources above minimum capital regulatory requirements and buffers) tended to lend less during the pandemic than those with more headroom.

However, it is unclear whether this reluctance to use capital buffers reflects banks' uncertainty regarding potential future losses or the wider market stigma that may result if a bank were to operate in its buffers.

Most authorities that maintained a positive countercyclical capital buffer (CCyB) prior to the pandemic reduced them in order to provide banks with additional headroom.

Similarly, several authorities that did not have positive CCyBs lowered other regulatory requirements or buffer levels.

While it is difficult to assess the quantitative effect of these capital releases independent of other measures, analysis provides some evidence that the capital release had a positive effect on lending during the pandemic.

These findings, taken together with supervisors' survey responses, suggest that it may be beneficial to consider whether there is sufficient releasable capital in place to address future systemic shocks.

The report also includes an analysis of price and yield movements of AT1 capital instruments compared to those of subordinated debt instruments and common equity.

The analysis indicates that the pandemic resulted in increased AT1 yield premia for both preferred stock and contingent convertible securities relative to unsecured debt, suggesting that market participants generally perceived AT1 instruments to be riskier than debt.

Furthermore, thus far during the pandemic, the two types of AT1 instruments have experienced broadly similar price movements indicating that investors do not perceive one instrument to be riskier than the other.

Regression analyses also show that AT1 prices are positively associated with both equity and subordinated long-term debt prices.

The report does not directly seek to address the issue of AT1 instruments' loss-absorption capacity on a going-concern basis.

Liquidity buffers

Certain banks faced liquidity pressure in the early phase of the pandemic. The severity of the pressure largely depended on banks' funding models. For example, banks reliant on unsecured wholesale money markets were more likely to have experienced pressure as funding sources dried up and they experienced large draws on loan facilities.

In contrast, banks with stable deposit franchises experienced negligible liquidity pressure even at the peak of the stress. While an increase in the amount of high-quality liquid assets that the Liquidity Coverage Ratio (LCR) requires banks to hold helped banks absorb this liquidity pressure, measures taken by central banks and governments to support economies significantly reduced liquidity pressures.

Overall, banks met large drawdown demands on committed lines and engaged in early buybacks of funding instruments from money market funds. Despite relatively limited liquidity stress, some jurisdictional studies

highlighted that a range of banks took defensive action, reflecting in part their targeting of internal LCR levels well above 100%.

However, these actions do not appear to have contributed materially to the wider disruption in financial markets that prompted central banks to intervene in March 2020.

The impact of the leverage ratio on financial intermediation

While the leverage ratio (which has not yet been implemented by all member jurisdictions) was not a binding constraint for most banks during the pandemic, the analysis – based on detailed jurisdictional studies – examines whether banks that had a smaller amount of capital above leverage ratio requirements and buffers were less active than other banks in financial market intermediation during the pandemic.

Overall, bank positions in government bond and repurchase agreement (repo) markets remained stable or rose in response to the rapid surge in client demand for liquidity at the onset of the crisis, though there is evidence that leverage ratio requirements may have reduced banks' incentives to mitigate the large imbalances that emerged in some markets.

Several member jurisdictions temporarily exempted central bank reserves from the leverage ratio calculation, which eased banks' balance sheet constraints on their intermediation activity.

To read more (95 pages) you may visit:
https://www.bis.org/bcbs/publ/d521.pdf

Number 3

Central bank digital currencies for cross-border payments Report to the G20, July 2021

Executive Summary

The G20 has made enhancing cross-border payments a priority and endorsed a comprehensive programme to address the key challenges.

Faster, cheaper, more transparent and more inclusive cross-border payment services would deliver widespread benefits for citizens and economies worldwide, supporting economic growth, international trade, global development and financial inclusion.

To that end, this report takes stock of the international dimension of central bank digital currency (CBDC, see glossary) projects and the extent to which they could be used for cross-border payments.

The report also investigates possible macro-financial implications associated with the cross-border use of CBDCs. The analysis does not imply that central banks mentioned in this report have reached a decision about issuance of a CBDC.

To date, no major jurisdiction has launched a CBDC and many design and policy decisions are still unresolved.

Also, most CBDC investigations by central banks focus on domestic issues and use cases.

Given this early state of play, the considerations in this report are exploratory and examine cross-border implications of CBDCs in a situation in which CBDCs are widely used.

In practice, domestic issuance of CBDC will be subject to considerable further economic and practical examination before exploration of cross-border use will gather pace.

Furthermore, enhancements in other areas of the cross-border payments programme, such as aligning regulatory, supervisory and oversight frameworks for cross-border payments, Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT)

consistency, Payment versus Payment (PvP) adoption and payment system access will be critical for cross-border CBDC use.

Against this background, the report identifies a number of questions that would need to be taken into account in order for CBDCs to support the enhancement of cross-border payments.

The report approaches these questions from two angles: first, from the practical perspective of how a cross-border payment infrastructure with CBDCs could be set up; and second, from a macro-financial perspective, examining the potential increase in cross-border flows, possible financial stability risks and currency substitution, and reserve currency configurations and backstops.

Cross-border payments with CBDCs can be envisioned in two fundamentally different ways. The first scenario assumes availability of a retail CBDC of a given jurisdiction to anybody inside and outside of that jurisdiction, with limited to no coordination between the issuing central banks.

In this case, if the design allows for anonymous payments like cash, it would by default be accessible to foreign residents. In practice, however, relatively few central banks are considering fully anonymous systems.

In contrast to cash, various restrictions on cross-border use could be imposed via the technological and regulatory design of the CBDC. This first scenario is conditioned by the domestic design of a CBDC.

The second scenario assumes some degree of interoperability between CBDCs based on access and settlement arrangements to facilitate the cross-border use of CBDCs from two or more jurisdictions.

Such arrangements can connect both wholesale and retail CBDCs across borders, imply strong cooperation among central banks, and include technological, market structure and legal aspects.

This second scenario – which is the main focus of the report – relies on design choices of the interoperability infrastructure.

Both scenarios are discussed in the report and illustrated with examples of ongoing projects.

Introducing a CBDC could have a range of macro-financial implications. Ultimately, those implications will depend on several factors, such as the

level and nature of international adoption, and on the degree of collaboration among issuing and recipient countries.

International use of CBDCs could potentially increase cross-border flows, but specific design choices of CBDCs could limit such use.

The implications would differ for wholesale versus retail CBDCs. Hence, multilateral collaboration to agree on design principles will be key to addressing concerns of central banks regarding currency substitution risk, capital flow volatility, and contagion risk.

These macro-financial implications of cross-border currency use are not exclusive for CBDCs, but also exist for privately issued forms of money.

However, CBDCs could allow jurisdictions greater room of manoeuvre to mitigate potentially adverse macro-financial implications.

CBDCs have the potential to enhance the efficiency of cross-border payments, as long as their design follows the “Hippocratic Oath for CBDC design” and its premise to “do no harm”, as highlighted by the Group of central banks (2020).

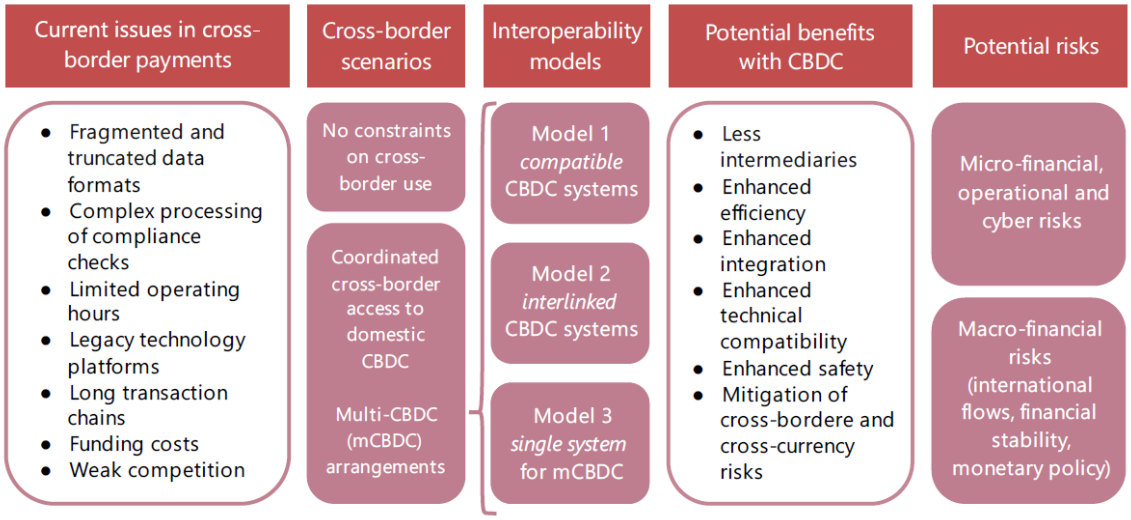
The coordination of national CBDC designs could lead to more efficient cross-currency and cross-border payments. Cross-border CBDCs could offer the opportunity to start with a “clean slate”, and address the frictions inherent in current cross-border payment systems and arrangements from the outset.

The enhancements could be made by offering secure settlement (see glossary), reducing costly and lengthy intermediation chains throughout the payment process, and eliminating operating hour mismatches by being accessible 24/7.

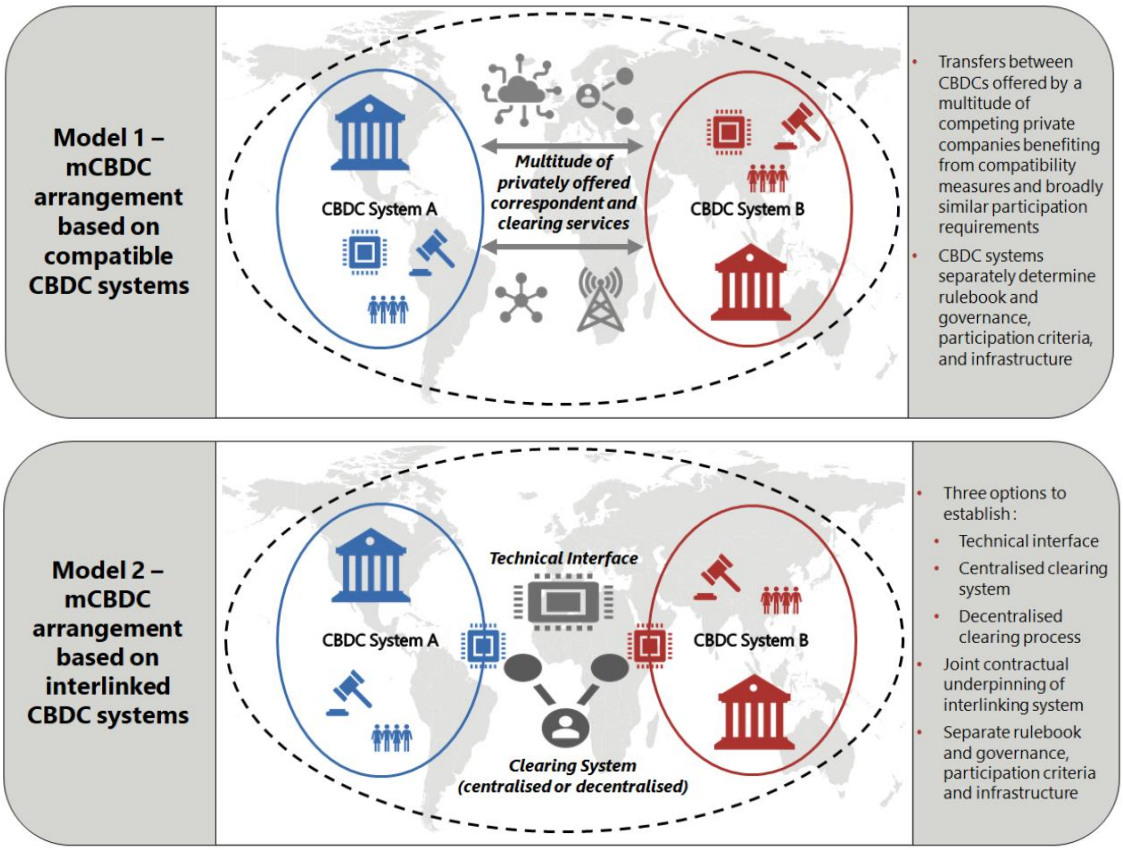
It is necessary to continue deepening the analysis on CBDC designs, especially regarding options for access and interlinking of CBDCs, including interoperability with non-CBDC payment infrastructures and arrangements.

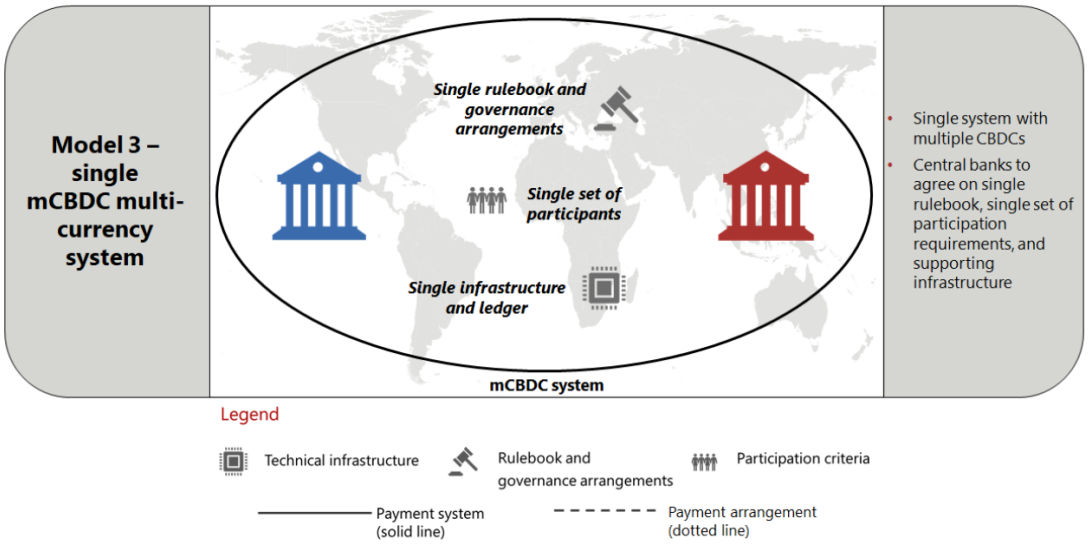
Further actions in this workstream will continue to investigate these questions, both from a practical and theoretical perspective and by leveraging analytical synergies from other building blocks of the cross-border programme, such as the investigation into global stablecoin arrangements and the feasibility of new multilateral platforms for cross-border payments.

Summary of the potential to enhance cross-border payments with CBDCs Graph 1



Source: CPMI; BIS Innovation Hub; IMF; World Bank.





Source: R Auer, P Haene and H Holden, "Multi-CBDC arrangements and the future of cross-border payments", *BIS Papers*, no 115, March 2021.

To read more: https://www.bis.org/publ/othp38.pdf

Number 4

Cyber espionage

Cyber espionage is considered both a threat and a motive in the cybersecurity playbook. It is defined as 'the use of computer networks to gain illicit access to confidential information, typically that held by a government or other organisation'.

In 2019, many reports revealed that global organisations consider cyber espionage (or nation-state-sponsored espionage) a growing threat affecting industrial sectors, as well as critical and strategic infrastructures across the world, including government ministries, railways, telecommunication providers, energy companies, hospitals and banks.

Cyber espionage focuses on driving geopolitics, and on stealing state and trade secrets, intellectual property rights and proprietary information in strategic fields. It also mobilises actors from the economy, industry and foreign intelligence services, as well as actors who work on their behalf.

In a recent report, threat intelligence analysts were not surprised to learn that 71% of organisations are treating cyber espionage and other threats as a 'black box' and are still learning about them.

In 2019, the number of nation-state-sponsored cyberattacks targeting the economy increased and it is likely to continue this way.

In detail, nation-state-sponsored and other adversary-driven attacks on the Industrial Internet of Things (IIoT) are increasing in the utilities, oil and natural gas (ONG), and manufacturing sectors.

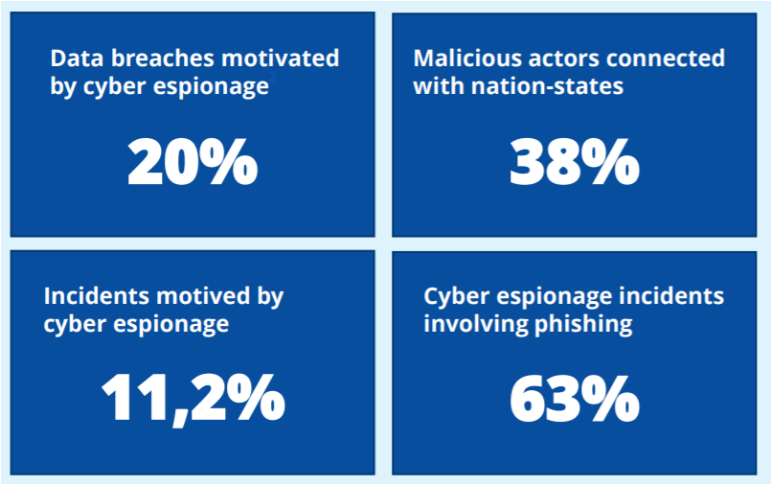
Furthermore, cyberattacks conducted by advanced persistent threat (APT) groups indicate that financial attacks are often motivated by espionage.

Using tactics, techniques and procedures (TTPs) akin to those of their espionage counterparts, groups such as the Cobalt Group, Carbanak and FIN7 have allegedly been targeting large financial institutions and restaurant chains successfully.

The European Parliament's Committee of Foreign Affairs called upon Member States to establish a cyber-defence unit and to work together on their common defence. It stated that 'the Union's strategic environment has been deteriorating ... in order to face the multiple

challenges that directly or indirectly affect the security of its Member States and its citizens; whereas issues that affect the security of EU citizens include: armed conflicts immediately to the east and south of the European continent and fragile states; terrorism – and in particular Jihadism –, cyberattacks and disinformation campaigns; foreign interference in European political and electoral processes'.

Threat actors motivated by financial, political, or ideological gain will increasingly focus attacks on supplier networks with weak cybersecurity programs. Cyber espionage adversaries have slowly shifted their attack patterns to exploiting third- and fourth-party supply chain partners.



To read the report:
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cyber-espionage

Number 5

Navigating the economy through the Covid crisis

Sir David Ramsden, Deputy Governor for Markets and Banking of the Bank of England, at The Strand Group, King's Business School.

Introduction

It's very good to be back speaking at this 51st Strand Group event and in my role as a Visiting Professor at King's. This is the third Strand Group event I've spoken at but my first time speaking to you virtually.

I've been involved in forecasting throughout my career, both in my current role as a Monetary Policy Committee (MPC) member and in my previous civil service career at HM Treasury.

Outside of work I'm also a keen mountain walker – most recently being lucky enough to spend some time on the Isle of Skye – and it's hard not to see parallels between the two activities.

Forecasts act as a map for policymakers of where the economy is heading, showing what adjustments to the current path are needed to avoid impending hazards and ensure they safely reach their policy objectives.

I should be clear at the outset, to borrow a well-worn quotation, that "the map is not the territory".

The forecast summarises what is likely to happen on the journey, but it is the economy itself that we as monetary policy makers must navigate, using the forecast alongside many other inputs, including a wide range of data and intelligence from the Bank's network of agents.

And as can sometimes happen when walking in the mountains, different MPC members can interpret the territory in different ways, supplementing the use of a map with the equivalent of a compass and GPS as well as their own judgement.

The job of economic forecasting has become increasingly tricky over recent years, as the economic territory underfoot has become less and less familiar.

The 2007-09 financial crisis was characterised by very large impacts on the supply side of the economy, as well as complex financial sector interactions and new forms of monetary stimulus in response.

That was followed the decade after by Brexit, which combined acute political and economic uncertainty with a multidimensional and shifting set of actual and anticipated impacts on demand, supply and the exchange rate.

And most recently we have had the Covid crisis, a one-in-ahundred-year health and economic crisis, which has left monetary policy makers firmly in unknown territory.

Of course the MPC have not been the only ones to find ourselves in this situation.

Other policy makers have faced similar challenges, and have found highly innovative and effective ways to overcome them, such as the Treasury's furlough scheme.

And of course the intellectual challenges faced by economic policy makers have been tiny compared with the very substantial challenges faced by the healthcare and other key workers who have had to tackle the Covid pandemic itself, as well as those who have suffered from the disease.

To read more: https://www.bis.org/review/r210715b.htm

https://www.bankofengland.co.uk/-/media/boe/files/speech/2021/july/navigating-the-economy-through-the-covid-crisis-speech-by-dave-ramsden.pdf?la=en&hash=67CB6432B2D51233D9CCC62F6F5D0DFD279C6E24

Number 6

A new strategy for a changing world

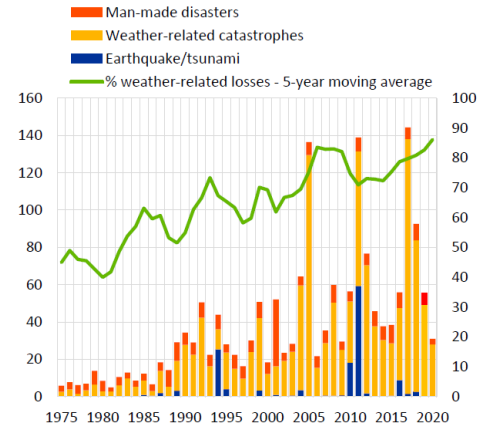
Isabel Schnabel, Member of the Executive Board of the European Central Bank, at a virtual event series, hosted by the Peterson Institute for International Economics.

Last week the Governing Council of the European Central Bank (ECB) published its new monetary policy strategy. It was the ECB's first review of its strategy since 2003, with most features of the framework still dating back to its founding years.

Since those times, the world economy has changed in fundamental ways.

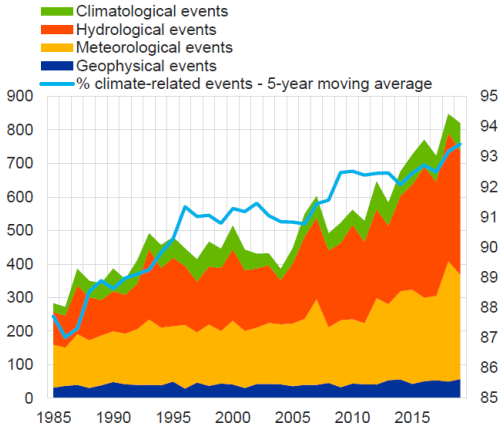
Rising physical risks of climate change

Global insured catastrophe losses
(left-hand scale: USD billions in 2020; right-hand scale: percentages)



Source: Swiss Re institute and ECB calculations.
Latest observation: June 2020.

Number of relevant natural loss events globally
(left-hand scale: number of events; right-hand scale: percentages)



Source: Munich Re NatCatService and ECB calculations.
Latest observations: December 2019.
Notes: Climatological events: drought and wildfire. Geophysical events: earthquake, tsunami, volcanic activity. Hydrological events: floods. Meteorological events: all types of storms.

About half of today's ten largest global firms by stock market capitalisation did not exist when the euro was launched in 1999.

In that year, imports accounted for around 30% of euro area economic activity; on the eve of the pandemic, this share had increased to 45%.

And whereas in 2000 there were on average 24 people aged 65 and over for every 100 persons of working age in the euro area, this ratio stood at 32 last year.

These changes reflect three broad macroeconomic trends – digitalisation, globalisation and demographic change – that have had, and continue to have, profound consequences for the conduct of monetary policy.

Amplified by the two deepest economic contractions since World War II – the global financial crisis and the coronavirus (COVID-19) pandemic – they shifted the challenge for monetary policy from fighting too high inflation towards preventing too low inflation, or even deflation, a phenomenon our previous strategy had not envisaged.

To read more:
https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp210714~0d62f657bc.en.html

The slides:
https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp210714_annex~7f2df0cedf.en.pdf

Number 7

China Requires Researchers to Report All Zero-Day Vulnerabilities

中共中央网络安全和信息化委员会办公室
Office of the Central Cyberspace Affairs Commission

The Cyberspace Administration of China (CAC) has issued new regulations that ask from security researchers to uncover critical flaws in computer systems and disclose them first-hand to the government authorities within two days of filing a report.

The new *"Regulations on the Management of Network Product Security Vulnerability"* will go into effect in September 2021.

You may visit: http://www.cac.gov.cn/

Number 8

Operation SpoofedScholars: report into Iranian APT activity

National Cyber Security Centre

Earlier this week, US cyber security company Proofpoint published a report into state-linked activity affecting the academic sector. The report: https://www.proofpoint.com/us/blog/threat-insight/operation-spoofedscholars-conversation-ta453?utm_source=social_organic&utm_social_network=twitter&utm_campaign=21_July_Corporate_blog+&utm_post_id=ccf4c45f-a244-4163-8b61-f55737f869ff

Key Takeaways

- TA453, an Iranian-state aligned actor, masqueraded as British scholars to covertly target individuals of intelligence interest to the Iranian government in what Proofpoint has dubbed Operation SpoofedScholars.
- The email conversations were benign until TA453 provided a link to a compromised website hosting a credential harvesting page.
- The use of a legitimate but actor-compromised website is an increase in sophistication compared to TA453's historical Tactics, Techniques, and Procedures of using actor-controlled credential phishing websites.
- Proofpoint has worked with the appropriate authorities to conduct victim notification.

Dubbed Operation SpoofedScholars, Proofpoint's findings show how actors masqueraded as British scholars to covertly target individuals of intelligence interest to the Iranian government.

Spear phishing campaigns by Iranian APT groups have been well documented in open-source reporting and Proofpoint notes a change in tactics for this threat group. Whilst these campaigns are targeted, they are broadly unsophisticated in nature.

The NCSC works closely with UK organisations across all economic sectors, including academia, to encourage better cyber resilience and raise awareness of the threats they face.

Our 2019 Cyber Threat to Universities report outlines risks and steps that can be taken to mitigate them. You may visit: https://www.ncsc.gov.uk/report/the-cyber-threat-to-universities

Number 9

Competition and collaboration: Understanding interacting epidemics can unlock better disease forecasts

A new algorithm increases scientists' abilities to accurately model mutually dependent spreading processes, from virus outbreaks to disinformation on social media, by Andrey Lokhov

Los Alamos NATIONAL LABORATORY

Epidemiological models took center stage throughout the COVID-19 pandemic, providing important information about the spread of the virus through communities and the world.

But the spotlight on these models also illuminated their shortcomings.

Early in the pandemic, several models were criticized for their lack of accuracy by either over or underestimating infection and death rates.

This is understandable given that, early on, little data was available to feed these models. As the pandemic progressed and more data became available, the better they got.

But the new epidemiological models are still far from perfect. A recently developed algorithm aims to improve them by focusing on additional forces critical to spread but too often overlooked.

Until now, epidemiological models that forecast how viruses spread through populations have struggled to include concepts of collaboration among various diseases themselves that, once in the human body, increase the chance of a co-infection.

For example, people living with HIV are 15 to 22 times more likely to get tuberculosis, and a person cannot contract hepatitis D unless they are already infected with hepatitis B.

To read more:
https://discover.lanl.gov/news/science-columns/discover-disease-forecasts

Number 10

NIST Evaluates Face Recognition Software's Accuracy for Flight Boarding

Agency's new test concerns checking in passengers and documenting their exit from a country.

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

The most accurate face recognition algorithms have demonstrated the capability to confirm airline passenger identities while making very few errors, according to recent tests of the software conducted at the National Institute of Standards and Technology (NIST).

The findings, released as *Face Recognition Vendor Test (FRVT) Part 7: Identification for Paperless Travel and Immigration (NISTIR 8381),* focus on face recognition (FR) algorithms' performance under a particular set of simulated circumstances: matching images of travelers to previously obtained photos of those travelers stored in a database. This use of FR is currently part of the onboarding process for international flights, both to confirm a passenger's identity for the airline's flight roster and also to record the passenger's official immigration exit from the United States.

The paper: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8381.pdf

NISTIR 8381

Face Recognition Vendor Test (FRVT)
Part 7: Identification for Paperless Travel and Immigration

The results indicate that several of the FR algorithms NIST tested could perform the task using a single scan of a passenger's face with 99.5% accuracy or better — especially if the database contains several images of the passenger.

"We ran simulations to characterize a system that is doing two jobs: identifying passengers at the gate and recording their exit for immigration,"

said Patrick Grother, a NIST computer scientist and one of the report's authors. "We found that accuracy varies across algorithms, but that modern algorithms generally perform better. If airlines use the more accurate ones, passengers can board many flights with no errors."

Previous FRVT studies have focused on evaluating how algorithms perform one of two different tasks that are among FR's most common applications. The first task, confirming that a photo matches a different one of the same person, is known as "one-to-one" matching and is commonly used for verification work, such as unlocking a smartphone. The second, determining whether the person in the photo has a match in a large database, is known as "one-to-many" matching.

This latest test concerns a specific application of one-to-many matching in airport transit settings, where travelers' faces are matched against a database of individuals who are all expected to be present. In this scenario, only a few hundred passengers board a given flight. However, NIST also looked at whether the technology could be viable elsewhere in the airport, specifically in the security line where perhaps 100 times more people might be expected during a certain time window. (The database was built from images used in previous FRVT studies, but the subjects were not wearing face masks.)

As with previous studies, the team used software that developers voluntarily submitted to NIST for evaluation. This time, the team only looked at software that was designed to perform the one-to-many matching task, evaluating a total of 29 algorithms.

Among the report's findings are:

The seven top-performing algorithms can successfully identify at least 99.5% of passengers the first time around if the database contains one image of a passenger. If the database contains a single image of each individual, the study shows that for as many as 428 of 567 simulated flight boarding processes, with each flight carrying 420 passengers, the most accurate FR algorithm can identify passengers for boarding without any false negatives (meaning the software fails to match two images of the same person). Stated in terms of error rates, this corresponds to at least 99.87% of travelers being able to board successfully after presenting themselves one time to the camera. Six additional algorithms give better than 99.5% accuracy.

Performance improves dramatically if the database contains multiple images of a passenger. The database gallery can contain more than one image of a single passenger. When an average of six prior images of a

passenger are in the gallery, then all algorithms realize large gains: The most accurate algorithm will check the identities of passengers on 545 of 567 flights without any errors, and at least 18 developers' algorithms are effective at identifying more than 99.5% of travelers accurately with a single presentation to the camera.

Demographic differences in the dataset have little effect. The team explored differences in performance on male versus female subjects and also across national origin, which were the two identifiers the photos included. National origin can, but does not always, reflect racial background. Algorithms performed with high accuracy across all these variations. False negatives, though slightly more common for women, were rare in all cases.

Grother said that the study does not address an important factor: the sort of camera that an FR system uses. Because airport environments differ, and because the cameras themselves operate in different ways, the report offers some guidance for tests that an airline or immigration authority could run to complement the NIST test results. Such tests would provide accuracy estimates that reflect the actual equipment and environment where it is used.

"We do not focus on cameras, which are an influential variable," he said. "We recommend that officials conduct the other tests we outline so as to refine their operations."

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.

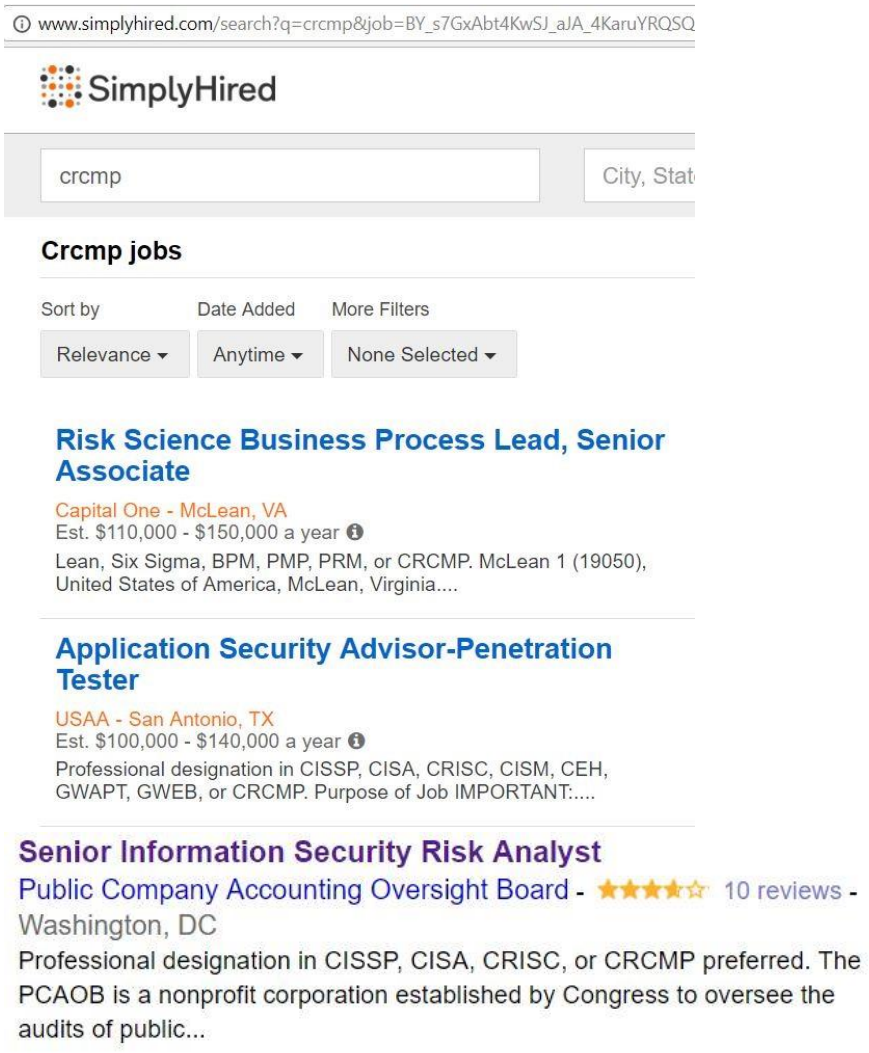
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

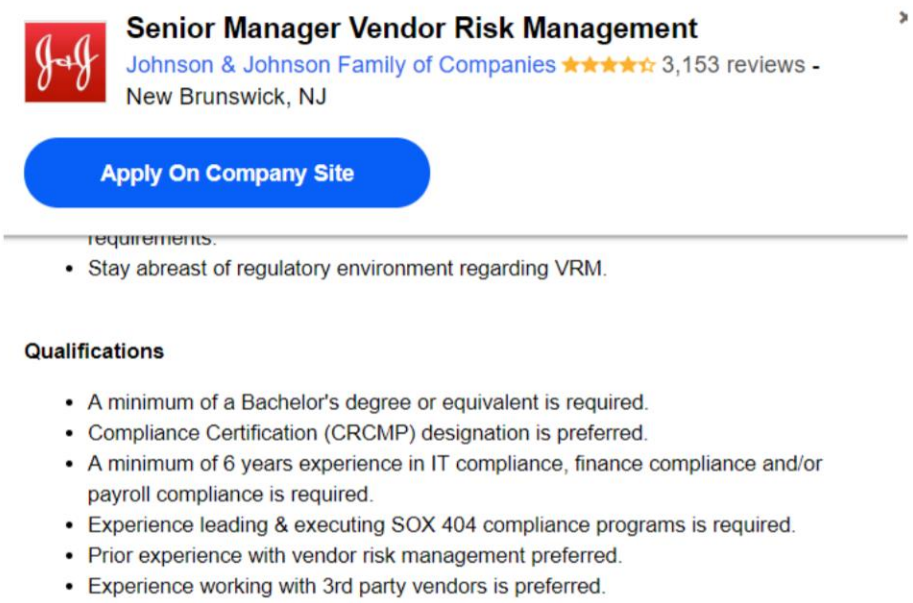
You can explore what we offer to our members:

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.





Senior Manager Vendor Risk Management

Johnson & Johnson Family of Companies ★★★★☆ 3,153 reviews -
New Brunswick, NJ

Apply On Company Site

requirements.

- Stay abreast of regulatory environment regarding VRM.

Qualifications

- A minimum of a Bachelor's degree or equivalent is required.
- Compliance Certification (CRCMP) designation is preferred.
- A minimum of 6 years experience in IT compliance, finance compliance and/or payroll compliance is required.
- Experience leading & executing SOX 404 compliance programs is required.
- Prior experience with vendor risk management preferred.
- Experience working with 3rd party vendors is preferred.

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.