International Association of Risk and Compliance Professionals (IARCP)
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA
Tel: 202-449-9750, Web: www.risk-compliance-association.com

Monday, January 24, 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,

According to the Financial Stability Oversight Council's *2021 Annual Report,* a destabilizing cybersecurity incident could potentially threaten the stability of the U.S. financial system through at least *three channels:*

First, the incident could disrupt a key financial service or utility for which there is little or no substitute. This could include attacks on central banks; exchanges; sovereign and subsovereign creditors, including U.S. state and local governments; custodian banks, payment clearing and settlement systems; or other firms or services that lack substitutes or are sole service providers.

Second, the incident could compromise the integrity of critical data. Accurate and usable information is critical to the stable functioning of financial firms and the system; if such data is corrupted on a sufficiently large scale, it could disrupt the functioning of the system. The loss of such

data also has privacy implications for consumers and could lead to identity theft and fraud, which in turn could result in a loss of confidence.

Third, a cybersecurity incident that causes a loss of confidence among a broad set of customers or market participants could cause customers or participants to question the safety or liquidity of their assets or transactions, and lead to significant withdrawal of assets or activity.

According to the report, a greater prevalence of teleworking compared with the pre-pandemic period could result in vulnerabilities from that source remaining elevated. The implementation of teleworking strategies using virtual private networks, virtual conferencing services, and other technologies can increase cybersecurity vulnerabilities, *insider risks,* and other operational exposures.

Firms have *increased their reliance* on third-party service providers to implement these strategies, and for a variety of other services as well.

The interdependency of networks and technologies supporting critical operations magnifies cyber risks, threatening the operational capabilities of individual institutions and the financial sector as a whole.

Rapid adoption of new technologies and interconnected platforms used to support hybrid work models have enhanced the efficient provision of financial services but have simultaneously increased complexity of information technology and operations.

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

Best regards,

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

Number 8 (Page 25)

Digital currencies and the soul of money

Agustín Carstens, General Manager of the BIS, Goethe University's Institute for Law and Finance (ILF) conference on "Data, Digitalization, the New Finance and Central Bank Digital Currencies: The Future of Banking and Money".

Number 9 (Page 34)

Europol's Statement on the Decision of the European Data Protection Supervisor

Number 10 (Page 36)

Department of Homeland Security Announces Climate Change Professionals Program

Number 1

Asset quality has further improved, but cyber risk remains a source of concern for EU banks

- Bank capital ratios remain well above regulatory requirements.

- Asset quality has further improved, but there are concerns for loans that have benefited from moratoria and public guarantee schemes not least due to general uncertainty due to Covid-19 variant, Omicron.

- Profitability has stabilised at levels above those seen before the pandemic.

- The majority of banks expect a rise in operational risks mainly due to elevated cyber risks.

The European Banking Authority (EBA) today published its quarterly Risk Dashboard together with the results of the autumn edition of the Risk Assessment Questionnaire (RAQ).

The NPL ratio declined to 2.1% and the stage 2 ratio contracted to 8.7%.

Return on equity (RoE) was reported higher than pre-pandemic levels at 7.7%.

RAQ results show that around 50% of banks cover their cost of equity (CoE) with more than 70% of banks estimate a CoE range between 8% and 12%.

It remains to be seen to what extent the Omicron-related wave of infections will affect asset quality and profitability.

The CET1 ratio reached 15.4% on a fully loaded basis in Q3 2021. It declined by 10bps due to a small decrease in capital combined with a slight increase in risk weighted assets (RWA).

There is however significant variation in CET1 ratios across banks with the interquartile range spanning from 14.1% to 20%.

The leverage ratio remained unchanged at 5.7% on a fully loaded basis.

The decline in the NPL ratio (20bps QoQ) was driven by a 5% decrease in NPLs to EUR 419bn and was broad based.

The NPL ratio for household exposures declined to 2.5% (2.7% in Q2) and for loans towards non-financial corporates (NFCs) to 4.2% (4.4% in Q2).

The sectors more vulnerable to Covid-related measures continue to have higher NPL levels but have also shown improvement.

For example, the NPL ratio of accommodation and food service activities decreased by 20bps to 9.5% and for arts, entertainment, and recreation by 50bps to 7.7%.

The rising trend observed in the volume of forborne loans since the beginning of the pandemic halted at around EUR 383bn (2.0% of total loans).

Loan volumes under current moratoria decreased further. The volume of loans under existing moratoria was EUR 50bn (around EUR 125bn in Q2), with around a third (33.6%) of them classified as stage 2 (28.1% in Q2) and 6% as NPLs (4.5% in Q2).

23.9% and 4.9% of loans with expired moratoria were reported under stage 2 and as NPL respectively (24.5% and 4.7% in Q2).

The total volume of loans under public guarantee schemes (PGS) reached EUR 378bn in Q3, unchanged compared to the last quarters.

20.1% them were under stage 2 and 2.4% were classified as NPLs (18.5% and 2% in Q2 respectively).

Low impairments supported profitability which is higher than pre-pandemic.

The RoE was reported at 7.7% (2.5% in Q3 2020 and 6.6% in Q3 2019).

Cost of risk was 0.47%, substantially lower than at the same period last year (0.74%) and at the same level as December 2019.

The downward trend of the net interest margin (NIM) stopped.

Net interest income (NII) continues to be the main contributor to banks' net operating income (55.4%), yet net fee and commission income has an increasing relevance (31.9%, up from 30.2% in Q3 2020 and 28.5% in Q4 2019).

The latter remains one of banks' key target areas to improve profitability in future, according to RAQ results.

The questionnaire's results also show that the share of banks charging negative rates to NFCs continued to rise (60% vs 55% before) whereas the share of banks charging negative rates to households remains stable at around 15%. The liquidity coverage ratio (LCR) stood at nearly unchanged 174.7%.

The decreasing trend of the loan to deposit ratio was uninterrupted and the ratio was 108.2% (108.9% in Q2 2021), driven by a higher rise of deposits towards NFCs and households rather than loans.

On banks' funding, RAQ results indicate that banks will focus on senior non-preferred/senior HoldCo (more than 50%) and preferred senior unsecured debt (35%) over the coming 12 months.

A smaller share of banks (25%) reports their intention to draw secured funding (covered bonds). Related to operational risks, a significant share of banks (55%) expects its increase, in line with previous surveys.

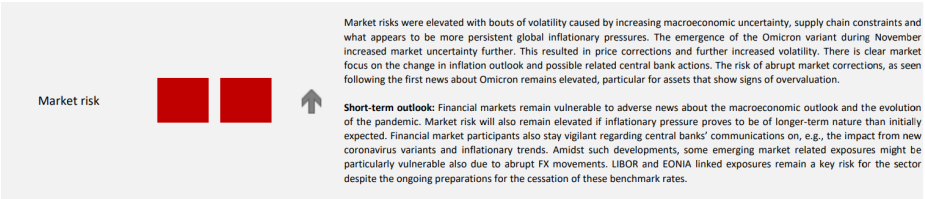
Of these banks, 90% consider cyber risk and data security issues, and around 40% cite conduct and legal risk as the main reasons for the expected increase in operational risk.

Banks reported in the RAQ that ESG factors are widely considered in their risk management. 80% of banks are taking them into account in credit risk, while more than 70% of banks consider them for reputational and operational risks.

The metrics most used by banks to assess their exposures to climate-related risks are carbon or greenhouse gas (GHG) financed emissions and environmental scores/ratings of counterparties (both indicated by 45% of banks).

They are followed by the share of green exposures (40%) and the share of environmentally harmful exposures (30%).

To read more:
https://www.eba.europa.eu/sites/default/documents/files/document_library/Risk%20Analysis%20and%20Data/Risk%20dashboard/Q3%202021/1025829/EBA%20Dashboard%20-%20Q3%202021%20v2.pdf



Number 2

Financial Stability Oversight Council
2021 Annual Report

The Financial Stability Oversight Council (Council) unanimously approved its 2021 annual report. This year's report describes activities of the Council over the past year, as the U.S. economy has continued to rebound from the disruptions caused by the COVID-19 pandemic.

Monetary and fiscal policy, substantial progress in vaccinations, and broadly accommodative financing conditions have together supported this recovery and bolstered the financial condition of households and businesses.

Additionally, the Council's annual report describes significant financial market and regulatory developments, potential emerging threats to U.S. financial stability, and recommendations to promote U.S. financial stability. The report was developed collaboratively by members of the Council and their agencies and staffs.

"The Financial Stability Oversight Council's annual report analyzes past episodes of financial turmoil to understand weak points in our financial system. It also reviews the actions taken by the Council to strengthen our financial system, with one eye on the past and one on the future," Secretary of the Treasury Janet L. Yellen said. "In the coming year, the Council will continue to monitor threats to financial stability and take concrete action where appropriate."

The Council's recommendations in the annual report include the following, among others:

- **Climate-related Financial Risk:** The Council recognizes the critical importance of taking prompt action to improve the availability of data and measurement tools, enhance assessments of climate-related financial risks and vulnerabilities, and incorporate climate-related risks into risk management practices and supervisory expectations for regulated entities, where appropriate.

  In addition, financial regulators, consistent with their mandates and authorities, should promote consistent, comparable, and decision-useful disclosures that allow investors and financial institutions to take climate-related financial risks into account in their investment and lending decisions. Through these actions, financial regulators can both promote financial-sector resilience and help the financial system support an orderly economy-wide transition to net-zero emissions.

- **Digital Assets:** The Council recommends that federal and state regulators continue to examine risks to the financial system posed by new and emerging uses of digital assets and coordinate to address potential issues that arise from digital assets. The Council recommends that member agencies consider the recommendations in the Report on Stablecoins published by the President's Working Group on Financial Markets, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency on November 1, 2021 (PWG Report).

  The Council will further assess and monitor the potential risks of stablecoins and recommends that its members consider appropriate actions within each member's jurisdiction to address those risks while continuing to coordinate and collaborate on issues of common interest. The Council will also be prepared to consider steps available to it to address risks outlined in the PWG Report in the event comprehensive legislation is not enacted.

- **LIBOR Transition:** Market participants should act with urgency to address their existing LIBOR exposures and transition to robust and sustainable alternative rates. The Council commends the efforts of the Alternative Reference Rates Committee and recommends that it continue to facilitate an orderly transition to alternative reference rates.

  Member agencies should determine whether regulatory relief is necessary to encourage market participants to address legacy LIBOR portfolios. Member agencies should also continue to use their

supervisory authority to understand the status of regulated entities' transition from LIBOR, including their legacy LIBOR exposure and plans to address that exposure.

- **Cybersecurity:** The Council recommends that federal and state agencies continue to monitor cybersecurity risks and conduct cybersecurity examinations of financial institutions and financial infrastructures to ensure, among other things, robust and comprehensive cybersecurity monitoring, especially in light of new risks posed by the pandemic, ransomware incidents, and supply chain attacks.

The report:
https://home.treasury.gov/system/files/261/FSOC2021AnnualReport.pdf

Number 3

Project Helvetia Phase II: Settling tokenised assets in wholesale CBDC

Project Helvetia was a multi-phase investigation by the BIS Innovation Hub, the Swiss National Bank (SNB) and the financial infrastructure operator SIX.

Project Helvetia Phase II was concluded in January 2022. It demonstrated that a wholesale central bank digital currency (wCBDC) **can be integrated** with existing core banking systems and processes of commercial and central banks. Furthermore, it showed that issuing a wCBDC on a distributed ledger technology (DLT) platform operated and owned by a private sector company is feasible under Swiss law.

The experiment – conducted together with five commercial banks – explored the settlement of interbank, monetary policy and cross-border transactions on the test systems of SIX Digital Exchange (SDX), the Swiss real-time gross settlement system – SIX Interbank Clearing (SIC) – and core banking systems.

Project Helvetia is purely experimental and does not indicate that the SNB intends to issue wCBDC.

BIS Innovation Hub

"Tokenisation and distributed ledger technology (DLT) could bring significant changes to the financial system.

Phase I of Project Helvetia showed that wholesale central bank digital currency (wCBDC) can be used to settle tokenised assets in central bank money.

Phase II – as described in this report – expanded on the practical complexities, legal questions and policy implications of issuing wCBDC.

Phase II showcased the continued collaboration between the Swiss National Bank, SIX and the BIS Innovation Hub, together with five commercial banks. Building on earlier work, it successfully demonstrated how infrastructures based on DLT can integrate and interoperate with a range of existing systems.

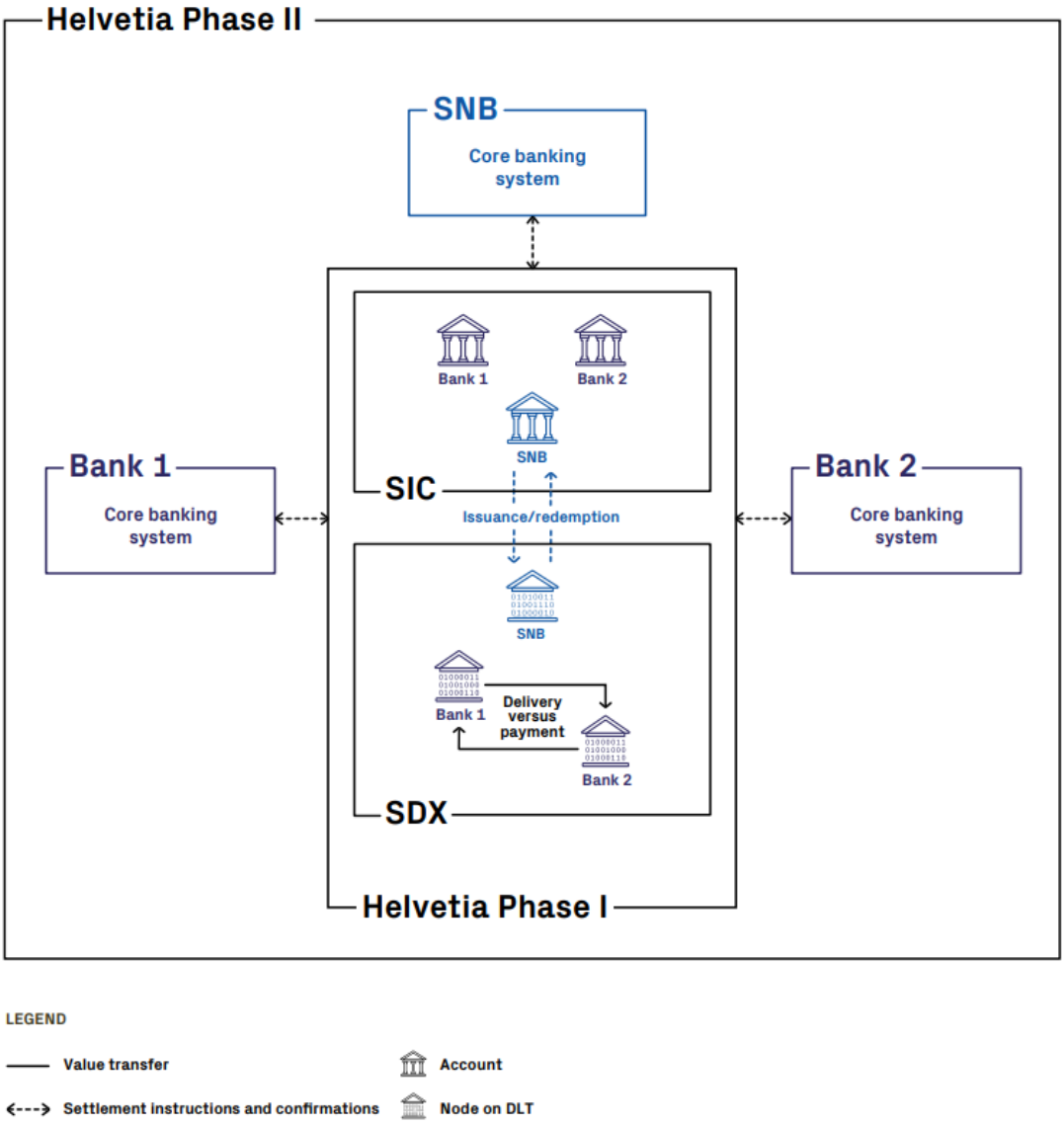
In this way, innovation is harnessed to preserve the best elements of the current financial system while also unlocking potential new benefits. As DLT goes mainstream, this will become more relevant than ever.

I wish to thank our partners for their excellent teamwork. The opportunities and challenges of innovation and interoperability in the financial ecosystem can only be addressed cooperatively.

Project Helvetia continued our demonstration of what the future could look like – and how we can work together to get there."

Benoît Cœuré
Head, BIS Innovation Hub

Graph 1: Overview of wCBDC experiment in Phase I and II



To read the paper: https://www.bis.org/publ/othp45.pdf

Number 4

Resolution Funding for Insurers, Practices paper

FSB FINANCIAL STABILITY BOARD

Table of Contents

Executive Summary

Resolution funding arrangements are essential to facilitate the effective and timely implementation of resolution measures.

Besides looking for sources of funding within the insurer or the group to which it belongs, resolution authorities tap on privately funded policyholder protection schemes (PPSs) or standalone resolution funds.

This practices paper on resolution funding ("Paper") looks at liquidity facilities available to insurers on a business-as-usual ("BAU") basis for them to manage their liquidity needs (e.g., the tri-party repo market in Switzerland) and presents examples of emergency liquidity assistance facilities that may be available to insurers (e.g., a liquidity line is available from the Deposit Insurance Corporation of Japan to a distressed insurer).

It also provides examples of sources of resolution funding in various jurisdictions.

In most jurisdictions, PPSs can not only be used for policyholder compensation when winding up an insurer but can also be used for funding portfolio transfers and run-offs which are common resolution actions.

In some others, standalone resolution funds exist and are funded on an ex-post basis, taking into consideration that such funds may have a limited scope of usage and an ex-ante funding could entail significant opportunity costs for the industry.

Some jurisdictions have both a PPS and a standalone resolution fund.

When resolving an insurer who is a PPS member, the PPS may be tapped upon first, before the resolution fund.

The Paper also discusses temporary funding sources for resolution funds.

The final section of the Paper describes mechanisms in place to recover funds used in resolution.

Policy makers and resolution authorities may use the Paper as reference as they develop their resolution funding framework for insurance.

Box 1.1: Insurance Groups with Banking Subsidiaries in France: Approach to Theoretical Liquidity Risks

Historically, the French landscape of financial institutions has been dominated by major financial conglomerates that conduct both insurance and banking activities during the past decades. Such financial conglomerates are known as “bancassurance” groups in France.

As large parts of the French insurance market belong to such bancassurance groups, particularly the life insurers, it could - at least in theory - expose insurers to banking liquidity risk. However, the parent company of most bancassurance groups is a bank (for which the recovery and resolution European banking regime applies) owning insurance subsidiaries that do not have high liquidity risks. On the contrary, insurance subsidiaries can provide the banking part of these groups with an additional stable source of liquidity, as demonstrated during the 2008 crisis.

Regarding most bancassurance groups whose parent company is an insurance company, it appears that their banking subsidiaries are typically not material. In this regard, it should be noted that the most significant insurance company in France is waived from supplementary supervision required for conglomerates. It does not need to comply with the financial conglomerates directive n°2002/87/EC on supplementary supervision of credit institutions, insurance undertakings and investment firms in a financial conglomerate. This is because it does not exceed the thresholds set out in the financial conglomerates directive to assess the significance of cross-sectoral activities. The situation is different for the six biggest banking groups, which are all conglomerates, since they are subject to the aforementioned supplementary supervision for conglomerates, and for which the European Central Bank (ECB) is the supervision coordinator.

Box 2.5: Netherlands' Resolution Fund

The goal of the resolution fund is to facilitate resolution of insurers. It is part of the Dutch resolution regime for insurers, which came into effect in 2019. It is funded ex-post by levies on the insurance sector. It can be used 1) to compensate creditors, including policyholders, in case the NCWOL safeguard has been violated; 2) to return to the bankrupt estate any pay-out from a failing insurer that has been deemed too high (i.e. during resolution, pay-outs can be made to policyholders for part of their pensions and annuities which they rely on for their day-to-day living. These pay-outs will prudently be based on expected outcome of the insolvency/resolution. In rare cases the pay-outs may turn out to have been too high, and detrimental to the other creditors. In that case the administrator/DNB will not claim back from policyholders the excess amounts paid to them. Instead the other creditors would be compensated using the resolution fund.); and 3) to cover operational costs of resolution, such as the establishment of a bridge institution. Because of its recent establishment, it has never been used yet.

The resolution fund cannot be used to absorb losses or capitalize a failing insurer. Insurer's deficits are for the account of shareholders and creditors. In the case of large deficits, policyholders may also lose some of the value of their insurance policies. Unlike in the case of banks, there is no guarantee scheme for policyholders. Instead, the resolution fund ensures that policyholders will never be worse off as a result of resolution than as a result of bankruptcy. This allows the resolution authority and the trustee to (partly) continue payments from the bankrupt estate to those policy holders that rely on these payments, after the insurer has failed, and helps transfer insurance portfolios (by covering operational costs of a bridge institution).

Other resolution costs are passed on to the insurance sector retrospectively, separately from the resolution fund. These may include costs for engaging the services of independent experts. DNB also passes the costs of regular resolution planning on to the insurance sector.

To read more: https://www.fsb.org/wp-content/uploads/P100122-1.pdf

Number 5

Shaping fair pay

BaFin Federal Financial Supervisory Authority

The amendment to the Remuneration Regulation for Institutions (Institutsvergütungsverordnung – InstitutsVergV) is in force, transposing further key remuneration provisions of CRD V into German law.

The amended Remuneration Regulation for Institutions entered into force on 25 September.

The primary purpose of the revision was to transpose into German law the remuneration rules of the fifth EU Capital Requirements Directive (CRD V) that the German Risk Reduction Act (Risikoreduzierungsgesetz – RiG) had not already transposed into the German Banking Act (Kreditwesengesetz – KWG) (see info box). As well as the provisions of CRD V, it also contains several clarifications and editorial amendments.

BaFin put the third and fourth regulations amending the Remuneration Regulation for Institutions (Institutsvergütungsverordnung – InstitutsVergV) out for consultation in November 2020.

The majority of the provisions implementing the remuneration requirements of CRD V are in the amending regulation that has now entered into force. The planned fourth amending regulation concerns only section 7 of the InstitutsVergV.

This is in connection with the new section 10j of the KWG, which will govern the leverage ratio buffer requirement. The plan is for the fourth amending regulation to enter into force at the beginning of 2023.

Key changes

A key reform is to remove leasing and factoring firms from the scope of the Remuneration Regulation for Institutions (section 1 (1) sentence 2 of the InstitutsVergV).

Furthermore, certain non-significant institutions that meet the criteria laid down in section 1 (3) sentence 2 of the InstitutsVergV are now required to apply specific requirements from the special section of the InstitutsVergV to the remuneration of their risk takers.

These criteria are based primarily on Article 4(1) no. 145(c) to (e) of the EU Capital Requirements Regulation (CRR), which contains the definition of

small and non-complex institutions. This extension was inevitable due to the requirements of Article 94(4)(a)(i) of CRD V.

General requirements

A new requirement for appropriate remuneration systems in accordance with section 5 (1) no. 6 of the InstitutsVergV is that these must now be gender neutral. There can be no gender-based pay discrimination for equal work or work of equal value. This is likewise a requirement of CRD V.

The disclosure requirement under section 16 of the InstitutsVergV was also modified to reflect the fact that all institutions are now required to identify risk takers.

As a result, institutions that are not classified as significant in accordance with section 1 (3c) of the KWG are required to disclose quantitative information on the total remuneration of all employees in addition to the disclosures to be provided under Article 450 in conjunction with Articles 433b and 433c of the CRR.

Institutions that in accordance with Article 433b(2) of the CRR are not required to disclose information under Article 450 of the CRR are likewise not subject to the disclosure requirements under section 16 of the InstitutsVergV.

Special requirements

Changes have also been made to the specific requirements of the Remuneration Regulation for Institutions.

For example, the deferral periods for the variable remuneration paid to risk takers were increased to a minimum of four to five years from a minimum of three to four years (section 20 (1) of the InstitutsVergV).

The deferral periods for management board members and management levels directly below them remain a minimum of five years.

Further amendments were made to the rules for groups of institutions. The new section 27 (1) sentence 1 of the InstitutsVergV requires that the group's parent undertaking establish a group-wide remuneration strategy.

This includes determining principles for remuneration systems that are appropriate, transparent, gender neutral and geared to the group's long-term development.

The remuneration strategy also applies to subordinated undertakings that are exempted from the specific remuneration provisions of the German Banking Act and the Remuneration Regulation for Institutions.

Section 27 (2) of the InstitutsVergV stipulates that significant institutions and non-significant institutions subject to one of the specific requirements under section 1 (3) sentence 2 of the InstitutsVergV must also identify group risk takers and apply the remuneration requirements to them in the applicable scope.

CRD V specifies that subsidiaries within the prudential scope of consolidation which are subject to sector-specific remuneration requirements may be excluded from the specific remuneration provisions.

This includes asset management companies, which to date in Germany had been exempted from applying the Remuneration Regulation for Institutions.

Under the new version of section 27 (3) of the InstitutsVergV, all other subsidiaries with sector-specific requirements can now be excluded, as can subsidiaries domiciled in a third country that would fall under sector-specific law had they been established in the EU.

To prevent institutions from transferring staff to such group entities in order to circumvent the Remuneration Regulation for Institutions, the new section 27 (4) of the InstitutsVergV prohibits exemptions from the remuneration requirements for staff whose professional activities have a material impact on the risk profile of an institution within the group.

Risk Reduction Act

The German Risk Reduction Act (Risikoreduzierungsgesetz – RiG), which entered into force at the end of 2020, transposed the remuneration rules of CRD V into the German Banking Act (Kreditwesengesetz – KWG).

A key change in the KWG was to expand the identification of risk takers to cover all institutions.

Now, institutions that are not classified as significant under section 1 (3c) of the KWG must also identify specific employee categories as risk takers (see sections 1 (21) and 25a (5b) sentence 1 of the KWG).

However, the duty to identify risk takers in accordance with Commission Delegated Regulation (EU) 2021/923 continues to apply solely to

institutions classified as significant in accordance with section 1 (3c) of the KWG (see section 25a (5b) sentences 2 and 3 of the KWG).

To read more:
https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2021/fa_bj_2110_InstitutsVergV_en.html

Number 6

BIS Board elects François Villeroy de Galhau as new Chair

The Board of Directors of the Bank for International Settlements (BIS) elected as its new Chair, François Villeroy de Galhau, Governor of the Bank of France. His term is for a period of three years, commencing on 12 January 2022.

Mr Villeroy de Galhau succeeds Jens Weidmann who served as Chair of the Board until the end of December 2021 when he concluded his tenure as President of the Deutsche Bundesbank.

Members of the Board of Directors expressed their sincere gratitude to Mr Weidmann for his excellent services to the Bank during his chairmanship.

The Board is responsible for determining the strategic and policy direction of the BIS, supervising its Management, and fulfilling the specific tasks given to it by the Bank's Statutes.

Board of Directors

The Board is responsible for determining the strategic and policy direction of the BIS, supervising BIS Management, and fulfilling the specific tasks given to it by the Bank's Statutes. It meets at least six times a year.

Composition of the Board

The Board may have up to 18 members, including six ex officio Directors, comprising the central bank Governors of Belgium, France, Germany, Italy, the United Kingdom and the United States.

They may jointly appoint one other member of the nationality of one of their central banks. Eleven Governors of other member central banks may be elected to the Board.

The Board elects a Chair and may elect a Vice-Chair from among its members, each for a three-year term.

Chair: François Villeroy de Galhau, Paris

Vice-Chair: Stefan Ingves, Stockholm

Roberto Campos Neto	Brasilia
Andrew Bailey	London
Shaktikanta Das	Mumbai
Thomas Jordan	Zurich
Klaas Knot	Amsterdam
Haruhiko Kuroda	Tokyo
Christine Lagarde	Frankfurt am Main
Juyeol Lee	Seoul
Tiff Macklem	Ottawa
Joachim Nagel	Frankfurt am Main
Jerome H Powell	Washington
Ignazio Visco	Rome
John C Williams	New York
Pierre Wunsch	Brussels
Yi Gang	Beijing

Number 7

Cybercriminals Tampering with QR Codes to Steal Victim Funds

The FBI is issuing this announcement to raise awareness of malicious Quick Response (QR) codes. Cybercriminals are tampering with QR codes to redirect victims to malicious sites that steal login and financial information.

A QR code is a square barcode that a smartphone camera can scan and read to provide quick access to a website, to prompt the download of an application, and to direct payment to an intended recipient.

Businesses use QR codes legitimately to provide convenient contactless access and have used them more frequently during the COVID-19 pandemic.

However, cybercriminals are taking advantage of this technology by directing QR code scans to malicious sites to steal victim data, embedding malware to gain access to the victim's device, and redirecting payment for cybercriminal use.

Cybercriminals tamper with both digital and physical QR codes to replace legitimate codes with malicious codes.

A victim scans what they think to be a legitimate code but the tampered code directs victims to a malicious site, which prompts them to enter login and financial information.

Access to this victim information gives the cybercriminal the ability to potentially steal funds through victim accounts.

Malicious QR codes may also contain embedded malware, allowing a criminal to gain access to the victim's mobile device and steal the victim's location as well as personal and financial information.

The cybercriminal can leverage the stolen financial information to withdraw funds from victim accounts.

Businesses and individuals also use QR codes to facilitate payment. A business provides customers with a QR code directing them to a site where they can complete a payment transaction. However, a cybercriminal can

replace the intended code with a tampered QR code and redirect the sender's payment for cybercriminal use.

While QR codes are not malicious in nature, it is important to practice caution when entering financial information as well as providing payment through a site navigated to through a QR code. Law enforcement cannot guarantee the recovery of lost funds after transfer.

TIPS TO PROTECT YOURSELF:

- Once you scan a QR code, check the URL to make sure it is the intended site and looks authentic. A malicious domain name may be similar to the intended URL but with typos or a misplaced letter.

- Practice caution when entering login, personal, or financial information from a site navigated to from a QR code.

- If scanning a physical QR code, ensure the code has not been tampered with, such as with a sticker placed on top of the original code.

- Do not download an app from a QR code. Use your phone's app store for a safer download.

- If you receive an email stating a payment failed from a company you recently made a purchase with and the company states you can only complete the payment through a QR code, call the company to verify. Locate the company's phone number through a trusted site rather than a number provided in the email.

- Do not download a QR code scanner app. This increases your risk of downloading malware onto your device. Most phones have a built-in scanner through the camera app.

- If you receive a QR code that you believe to be from someone you know, reach out to them through a known number or address to verify that the code is from them.

- Avoid making payments through a site navigated to from a QR code. Instead, manually enter a known and trusted URL to complete the payment.

Number 8

Digital currencies and the soul of money

Agustín Carstens, General Manager of the BIS, Goethe University's Institute for Law and Finance (ILF) conference on "Data, Digitalization, the New Finance and Central Bank Digital Currencies: The Future of Banking and Money".

I'd like to express my gratitude to the organisers for inviting me here today. It's an honour to deliver this speech at Goethe University. Of course, I wish I could have been in Frankfurt in person.

In a speech at this university four years ago, I addressed the growth and pitfalls of cryptocurrencies such as Bitcoin. Since then, the debate on the future of money has grown much broader, but it continues to touch on the very foundations of the monetary system.

Today I will take inspiration from your institution's namesake. The great Johann Wolfgang von Goethe was a well-travelled cosmopolitan and a true universalist. He was a poet and novelist, a playwright and theatre director, a scientist and statesman. Remarkably, his work anticipated some key economic issues of our time, including central bank independence.

Goethe's work confronts fundamental questions. In his masterpiece, Faust, he addresses the "Gretchenfrage" – a term that has become synonymous with a fundamental question of life.

For central bankers, the Gretchenfrage has always been: what is the soul of money? Today, technologists, innovators and futurists are offering new answers to this question. Some say that in the future, money and finance will be provided by just a few big tech corporations. Others dream of a decentralised system in which blockchains and algorithms replace people and institutions. And maybe, all of this will take place in the Metaverse.

My main message today is simple: the soul of money belongs neither to a big tech nor to an anonymous ledger. The soul of money is trust. So the question becomes: which institution is best placed to generate trust? I will argue that central banks have been and continue to be the institutions best placed to provide trust in the digital age. This is also the best way to ensure an efficient and inclusive financial system to the benefit of all.

Let me elaborate on this theme, starting with the institutional foundations of money.

The institutional foundations of money

Money is a societal convention. People accept money today with the expectation that everyone else will accept it tomorrow.

At its core, trust in the currency holds the monetary system together. Like the legal system, this trust is a public good. Maintaining it is crucial for the effective functioning of societies.

Trust requires sound institutions that can stand the test of time. Institutions that ensure the stability of the currency as the economy's key unit of account, store of value and medium of exchange, and that guarantee the safety and integrity of payments.

Throughout a history measured not in years but in centuries, independent central banks have emerged as the key institutions that underpins this trust in money. Alternatives have often ended badly.

It is for good reason that most countries have established central banks with a clear mandate to serve society. As public policy institutions, central banks have proven successful in upholding trust while adapting to societal and economic change.

In pursuing these mandates, central banks have managed to constantly adapt to technological, economic and societal changes. This is why central banks are actively engaging with digital innovation. They are working on new central bank public goods such as wholesale financial market infrastructures, retail fast payment systems and central bank digital currencies.

Of course, in a market-based system, the private sector remains the main engine of the economy. In today's two-tier monetary system, deposits are by far the most prevalent form of money held by the public, since cash holdings are relatively small. Banks, in turn, place their own deposits with the central bank as "bank reserves".

In this case, central banks provide an open, neutral, trusted and stable platform. Private companies use their ingenuity and dynamism to develop new payment methods and financial products and services. This combination has been a powerful driver of innovation and welfare.

But we cannot take this successful symbiosis for granted. Some recent developments may threaten money's essence as a public good, if taken too far.

To illustrate this, let me offer three plausible scenarios for the future of money.

- In the first, big tech stablecoins compete with national currencies and against each other too, fragmenting the monetary system.

- The second relates to the elusive promise of crypto and decentralised finance, or "DeFi", which claims to offer a financial system free from powerful intermediaries, but may actually deliver something very different.

- The third realises the vision of an open and global monetary and financial system that harnesses technology for the benefit of all.

You can probably guess which vision I espouse. I will close by discussing what it will take to achieve it.

Big tech stablecoins

Let's start with stablecoins issued by big techs. Stablecoins are cryptocurrencies that base their value on collateral, often in the form of deposits with commercial banks or other regulated financial instruments. They thus piggyback on the credibility of sovereign currencies. Stablecoins are issued in this first scenario by big techs, or large companies whose primary activity is digital services.

Big techs have made important contributions to financial services. Their new and innovative products have allowed hundreds of millions of new users into the formal financial system.

In the process, they have also achieved systemic relevance in several major economies. For example, big techs channel 94% of mobile payments in China.

This trend could accelerate if one of these firms were to grow in an unfettered way and create a dominant, closed ecosystem around its own global stablecoin.

Once established, a company is likely to erect barriers against new entrants, leading to market dominance, data concentration and reduced competition.

In addition, its stablecoin could disintermediate incumbent banks, which could even pose a risk to financial stability.

Moreover, if one big tech stablecoin takes hold, others will seek to imitate it. We may end up with a few dominant walled gardens that compete both with each other and with national currencies, thus fragmenting the national and global monetary systems. As the initial benefits fade, the well-known problems of market concentration will quickly follow.

In addition, the same economic forces that foster inclusion can also cause discrimination, privacy violations and market concentration. One reason is that data are subject to large externalities. For example, one person's data can reveal information about others.

Moreover, it is possible that the data holder ends up knowing more about users' behaviour than users do themselves. Armed with exclusive access to data, big techs can quickly scale up and dominate markets.

Let me be clear: it is undesirable to rely solely on private money. Users may initially find great convenience in paying with a big tech global stablecoin. But in doing so they may be handing the keys to our monetary system over to private entities, driven by profits and accountable only to their shareholders and other insiders. Such an arrangement could erode trust. A public good like money needs oversight with the public interest in mind.

The elusive promise of decentralization

A second plausible scenario for the future of money has attracted a growing number of enthusiasts. This vision replaces institutions with distributed ledger technology (DLT), in principle allowing anyone to be a validator in a shared network. It is embodied in the growth of cryptocurrencies and applications that build on them, such as so-called decentralised finance, or "DeFi".

DeFi's enthusiasts hold out some very appealing promises: DLT will "democratise finance", cutting out middlemen such as big banks. More generally, new decentralised protocols will lay the groundwork for "Web 3.0", or simply "web3". In this world, data will be reclaimed from the big techs, and entrepreneurs and artists will keep a greater share of the value they create.

Decentralisation can be a noble goal. In many applications, governance improves when power is genuinely dispersed, with appropriate checks and balances. This principle is embodied in free and competitive markets.

But this principle is not what DeFi applications are delivering. There is a large gulf between vision and reality.

To date, the DeFi space has been used primarily for speculative activities. Users invest, borrow and trade cryptoassets in a largely unregulated environment. The absence of controls such as know-your-customer (KYC) and anti-money laundering rules, might well be one important factor in DeFi's growth.

Indeed, a parallel financial system is emerging, revolving around two elements.

The first is automated, self-executing protocols, or "smart contracts". But these contracts will never be smart enough to cover every possible eventuality, and someone must therefore write and update the code, and run the platform. In practice, there is a lot of centralisation in DeFi. BIS economists have discussed this "decentralisation illusion" in recent research.

The second element is, again, stablecoins. These grease the wheels of DeFi. As they aim to maintain a fixed value to fiat currencies, they allow transfers across platforms, and form a bridge to the traditional financial system. Stablecoins are the settlement instrument in DeFi, alongside governance tokens and other more volatile cryptoassets.

But stablecoins may not be sound money. One drawback is the fact that they have to tie their value to regulated assets to borrow their credibility. Their issuers have an inherent incentive to invest reserve assets in a risky manner to earn a return. Without appropriate regulation, issuers can diverge from full backing, or test the margins of what counts as a safe asset – as experience has repeatedly shown.

More fundamentally, decentralisation comes at a cost. Trust in an anonymous system is maintained by self-interested validators who ensure the integrity of the ledger in the absence of a central authority.19 So the system must generate enough fees, or rents, to provide these validators with the right incentive.

These rents accumulate mostly to insiders, such as Bitcoin miners, or those who hold more governance tokens. These rents are also a reason why DeFi platforms have been so attractive for venture capital investment.21 Many protocols entrench insiders, as those with more coins have more power.

Ultimately, high rents for insiders mean high costs for users. So, while insiders who have sold coins to new users have made spectacular returns,

efficiency gains for average users have so far failed to materialise. And in the absence of regulation, fraud, hacks and so-called rug pulls have become rampant.

In addition, this structure makes it hard for fully decentralised systems to scale up. Achieving agreement in a large network takes time and effort, and consumes energy. The larger the ledger, the harder it becomes to update it quickly.

This is why many DLT systems can only handle a small volume of transactions to date, and often suffer from network congestion. This is also the reason why Bitcoin requires so much electricity. There are a variety of technical proposals to address this trade-off, but they all lead to greater complexity. Indeed, the need for rents to maintain incentives in a blockchain is a feature, not a bug; it is a case of "the more the sorrier" instead of "the more the merrier".

And the growing proliferation of different blockchains means that many competing candidates aim to be a single arbiter of truth.

Meanwhile, DeFi is subject to the same vulnerabilities as are present in traditional financial services. High leverage, liquidity mismatches and connections to the formal financial system mean vulnerabilities in DeFi could undermine the stability of the broader financial system.

As with money market mutual funds, there is a risk that, during a shock, stablecoins could face runs. With automated protocols, there may also be unpredictable interactions, as liquidity dries up and losses cascade through the system.

Thus, there is a risk that this "magic", once launched, may spin out of control. As in Goethe's Zauberlehrling ("The Sorcerer's Apprentice"), DeFi applications could take on a life of their own, interacting with one another in unpredictable ways. When a crash happens and money is lost, users will inevitably turn to a trusted and experienced party – the public authorities – to tame the unleashed spirits and restore order.

A better approach is possible. Building on sound money, new applications could stand on a stronger footing. They should not be based on anonymity but on identification and trust. And they should comply with financial regulation that is designed to keep the system safe.

Wherever private stablecoins are issued, they need to be adequately regulated to address the risks that they pose, such as runs, payment system

risk and concentration of economic power. We also need effective and consistent international policy on stablecoin arrangements.

Innovators should not fear regulators but work with them, to make their products more sound and more sustainable.

An open and global system as a public good

In a third scenario, incumbent financial institutions, big techs and new innovative entrants compete in an open marketplace that guarantees interoperability, building on central bank public goods. This means that end users can seamlessly interact across different providers – both domestically and across borders.

This would bring about continued innovation, and ever better outcomes for the economy as a whole. Trust in money remains the bedrock of stability. End users would see low costs and convenient services, with safety, privacy and a broad range of payment choices. This scenario harnesses the benefits of big data and DLT with market structures that foster competition and promote the public good nature of the monetary system.

In this vision, the monetary system is not fragmented into separate walled gardens, nor is it dominated by a few large corporations. There are also no high rents for insiders in anonymous networks.

At the core of this system are central banks. They do not aim for profits, but to serve society. They have no commercial interest in personal data. They act as operators, overseers and catalysts in payments markets, and regulate and supervise private providers in the public interest.

Working together, they can provide central bank digital currencies (CBDCs). Unlike stablecoins, CBDCs do not need to borrow their credibility. As they are directly issued by the central bank, they inherit the trust that the public already places in their currency. They can thus serve as a sound foundation for future innovation.

Central banks can provide this foundation domestically, but also on a global scale.

Imagine a global network of CBDCs. Different central banks would design and issue a new form of public money, tailored to their economies and societies' preferences.

Importantly, central banks could work with one another, and with the private sector, to ensure that these domestic CBDCs are interoperable

across borders. This would require technical compatibility, the ability for systems to "speak each other's language" and agreement on rights and obligations.

To obtain this, central banks could choose whether to build a network of bilateral links, or they could adopt a hub-and-spoke model or a single common platform. DLT could be used to connect multiple CBDCs issued by different central banks. This would be useful as no single central bank could straddle all the different currencies in the system.

Such a network would be a global version of domestic monetary systems grounded in the trust placed in central banks. It could lower the cost of cross-border payments; increase their speed and transparency; and broaden access to users in different countries. Private providers could interact with clients, conducting know-your-customer and other compliance checks.

The private sector could build a host of financial services on top of such a system, from innovative payments to lending, to insurance and investment services. But safeguards can give users control over personal data. This does not require the selling of speculative coins that serve only to enrich insiders.

The BIS Innovation Hub is working actively to make this vision a reality, with several experiments involving cooperation between central banks and the private sector. What is notable is that many of these projects are based on DLT, where the central banks play the key role.

Based on trust instead of rents, these systems overcome the inherent issues with scaling up. They also offer greater safety and efficiency. Three important BIS Innovation Hub projects all make use of a DLT platform upon which multiple central banks issue their own wholesale CBDCs so that they can be traded between participants to enable faster, cheaper and safer cross-border settlements.

- In Project Jura, each central bank maintains individual control over its own CBDC on a single platform with separate subnetworks.

- In project mBridge, each participating central bank issues its own CBDCs and operates a validating node in a shared system.

- Project Dunbar explores the advantages and disadvantages of different DLT prototypes and validating mechanisms to support a common multi-CBDC platform.

Overall, these projects show that there is significant potential in new technologies, including DLT, if they are applied in a way that builds on the monetary system's existing institutional framework. Central banks, as validating nodes, are not there to make money by mining coins. Instead, they perform this role as part of their public service mandate.

Working in a controlled environment and with industry partners, the BIS and host central banks are developing public goods that can be thoroughly tested and ready to be rolled out in the real world.

Conclusion

Let me conclude. The future of money is ours to shape. While central banks share the excitement around digital innovation, we are aware of the potential consequences of some of its incarnations.

The design of money has consequences that concern all of society: the integrity and stability of money and payments, market concentration, consumer rights and efficiency. Hence, central bankers must work with other public authorities and private stakeholders to make the vision I have described a reality.

Let's innovate in a sound, sustainable way, harnessing the benefits of digital technology in a way that is consistent with our shared values. In particular, let's ensure that our financial system builds on the existing governance of money, serves the public interest, and works cooperatively with the private sector.

So, let me go back to where I started, to Goethe. The answer to the Gretchenfrage has not changed: central banks and public authorities are still the glue that holds the monetary and financial system together. Private sector services and innovation are essential and should thrive on this foundation. But trust can never be outsourced nor automated.

Herzlichen Dank für Ihre Aufmerksamkeit!

You may visit: https://www.bis.org/speeches/sp220118.htm
The video: https://www.youtube.com/watch?v=YtC26lYhrQY

Number 9

Europol's Statement on the Decision of the European Data Protection Supervisor

Committed to the highest standards of data protection, Europol first reached out proactively to the European Data Protection Supervisor (EDPS) on 1 of April 2019 to seek guidance on the processing of large and complex datasets which are collected in lawful, judicial investigations.

Europol is increasingly receiving from its Member States datasets to help with their processing and analysis.

Since then, Europol has followed the guidance given by the EDPS and has kept its Management Board updated on the progress achieved.

Yesterday, the EDPS published his Decision on the retention of datasets without Data Subject Categorisation (DSC) by Europol. The DSC is the act of identifying in these datasets suspects, potential future criminals, contacts and associates, victims, witnesses and informants linked to criminal activities.

According to the EDPS, Europol should complete the DSC for large and complex datasets within a fixed retention timeline. In this context, the EDPS has highlighted that the current Europol Regulation does not contain an explicit provision regarding a maximum time period to determine the DSC.

In his decision the EDPS sets that this period must be of six months, at the expiry of which he requests Europol to erase the data.

The EDPS Decision will impact Europol's ability to analyse complex and large datasets at the request of EU law enforcement. This concerns data owned by EU Member States and operational partners and provided to Europol in connection with investigations supported within its mandate. It includes terrorism, cybercrime, international drugs trafficking and child abuse, amongst others.

Europol's work frequently entails a period longer than six months, as do the police investigations it supports. This is illustrated by some of Europol's most prominent cases in recent years.

Europol will seek the guidance of its Management Board and will assess the EDPS Decision and its potential consequences for the Agency's remit, for

ongoing investigations as well as the possible negative impact on the security for EU citizens.

Is Europol a European FBI?

No. Europol has no executive powers.

The European Police Office is a support service for the law enforcement agencies of the EU Member States. This means that Europol officials are not entitled to arrest suspects or act without the approval of national authorities. However, the support provided by Europol consists of tools that can contribute to the executive measures carried out by the relevant national authorities.

Number 10

Department of Homeland Security Announces Climate Change Professionals Program

The Department of Homeland Security (DHS) announced the creation of a new Climate Change Professionals Program to recruit recent graduates and current federal employees to support the Department's growing focus on adapting to climate change and improving resilience.

The program is one of many new activities under the umbrella of the DHS Climate Change Action Group, established in 2021 by Secretary Alejandro N. Mayorkas.

"The Climate Change Professionals Program will be instrumental in helping the Department adapt to our changing climate by providing hands-on experience and guidance to young professionals interested in climate adaptation and resilience," said Secretary Mayorkas. "This program will develop the next generation of climate experts, improve climate literacy throughout the Department, and help us execute our Climate Action Plan to remain mission-resilient while reducing our own impacts on the environment."

This two-year program will be run by the DHS Office of the Chief Readiness Support Officer and provide participants with hands-on opportunities to contribute to new initiatives that have the potential to substantially help DHS adapt to climate change and improve resilience.

Upon successful completion of the program, participants will receive a Climate Change Professional accreditation from the Association of Climate Change Officers and be eligible for permanent, full-time positions at DHS.

Participants in the program will work under the leadership of the Climate Change Action Group. The CCAG is comprised of senior officials from across the Department and focuses on promoting resilience and addressing multiple climate change-related risks, including flooding, extreme heat, drought, and wildfires.

The Climate Change Professionals Program is part of the Secretary's Honors Program, which was launched in July 2021 to recruit recent graduates and current federal employees with degrees in relevant fields for professional development programs at DHS.

Climate change is the second field included in the Secretary's Honors Program, following the launch of the cybersecurity program last year.

Interested applicants can view the first job postings for the Climate Change Professionals Program on the DHS is Hiring webpage. You may visit: https://www.dhs.gov/homeland-security-careers/hiring-event

DHS is Hiring

The Department of Homeland Security has a vital mission to secure the nation from the many threats we face. This requires the dedication of more than 230,000 employees in jobs that range from aviation and border security to emergency response, from cybersecurity analysis to chemical facility inspections. Our primary goal is clear - keeping America safe.

We are currently seeking exceptional candidates to fill mission critical positions in the areas of:

- Cybersecurity
- Information Technology
- Intelligence
- Law Enforcement
- Business Operations/Mission Support
- Immigration
- Travel Security
- Prevention and Response
- Emergency Management

To learn more about DHS's climate commitment, visit DHS Actions: Climate Change. You may visit: https://www.dhs.gov/dhs-actions-climate-change

The DHS Climate Action Plan includes five priority actions:

1. **Incorporating climate adaptation into national preparedness and community grants and projects,** including through the continuation of the Building Resilient Infrastructure and Communities (BRIC) program – the funding for which President Biden doubled to $1 billion – to provide incentives for state, local, tribal, and territorial governments to adopt modern, disaster-resistant building codes. DHS initial BRIC selections include wildfire resilience programs, flood control programs, and small-town coastal hazard mitigation plans.
2. **Incorporating climate adaptation planning and processes into homeland security mission areas,** including by reviewing current budget planning policies to assess whether climate change considerations are appropriately incorporated.
3. **Creating climate-resilient facilities and infrastructure,** including by aiming to electrify 50 percent of the DHS vehicle fleet by 2030.
4. **Ensuring climate-ready services and supplies,** for both the Department and the Nation, including by using CISA's national risk assessment program to assess climate impacts and adaptation strategies to secure supplies of food, medicine, energy, and other vital resources.
5. **Increasing climate literacy,** including by developing and implementing a DHS-wide climate education plan to raise awareness among our employees about the climate crisis and how to combat it through adaptation and resilience strategies.

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.

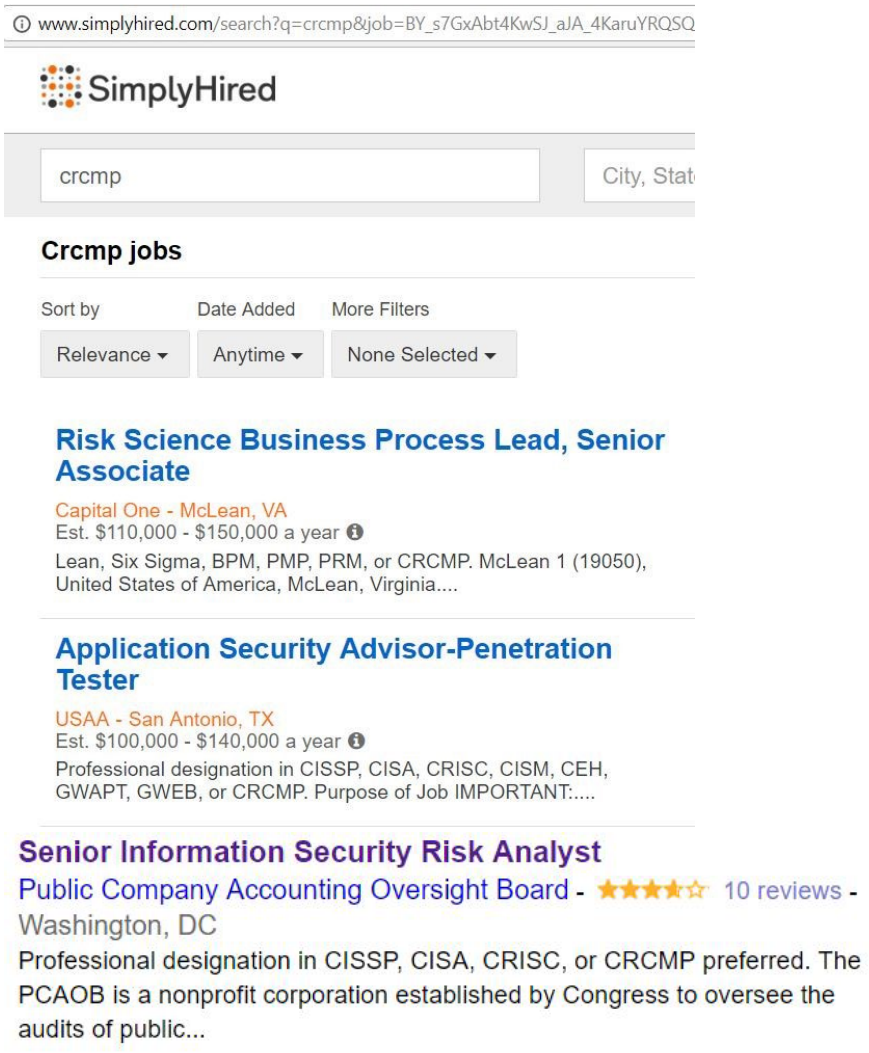
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

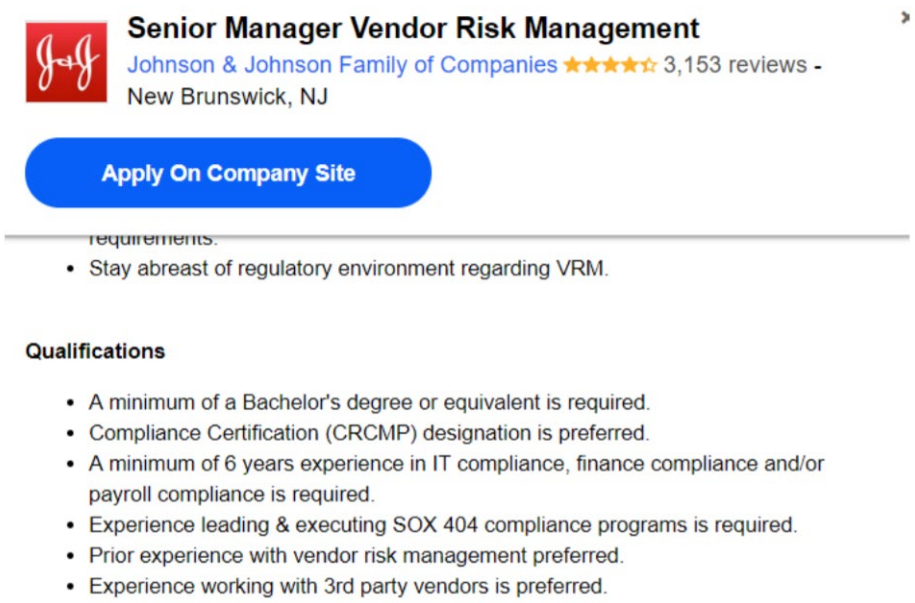
You can explore what we offer to our members:

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.

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