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, November 8, 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,

Friedrich Nietzsche believed that whoever fights monsters should be careful that in the process he does not become a monster. And if you gaze long enough into an abyss, the abyss will gaze back into you.

Cybersecurity is becoming more complex by the day. In the new *European Commission Work Programme 2022* (Communication from the Commission to the European Parliament and the Council) we read:

"The pandemic has served as a catalyst for the accelerating digitalisation of Europe and the world. The Commission will follow up on its path to the digital decade to deliver on the EU's digital transformation by 2030.

We are determined to lead the way in the global race for trustworthy, secure and human-centric technology. And we will work to reach agreement on

and implement our proposals for a safe and secure internet, a European digital identity and on trustworthy Artificial Intelligence.

With the economy and society relying more and more on digital solutions, we need to ensure that we can defend ourselves in a world increasingly prone to hacking of connected products and associated services.

To this end, we will propose a European Cyber Resilience Act to establish common cybersecurity standards for products. We will also begin building an EU space-based global secure communications system, offering EU-wide broadband connectivity where it currently does not exist and secure and independent communications to Member States."

This is very interesting. We will have another law for cybersecurity, the European Cyber Resilience Act.

The communication continues: "Our better regulation agenda ensures that political decisions are taken based on the best available evidence, taking into account the impact they will have on the ground and the views of people and businesses likely to be affected. This approach helps ensure that regulation is targeted, easy to comply with and does not add unnecessary regulatory burdens."

This "easy to comply with" is the joke of the day, in my opinion.

Best regards,

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

Number 1 (Page 5)

Cybersecurity in 2022 Commission Work Programme

Number 2 (Page 8)

Big techs in finance: on the new nexus between data privacy and competition

Number 3 (Page 11)

FSB Chair's letter to G20 Finance Ministers and Central Bank Governors

Number 4 (Page 14)

How Long is Too Long? How High is Too High?: Managing Recent Inflation Developments within the FOMC's Monetary Policy Framework

Governor Randal K. Quarles, at the 2021 Milken Institute Global Conference "Charting a New Course," Beverly Hills, California

Number 5 (Page 18)

Forum for Auditors of Small Businesses and Broker-Dealers

PCAOB Acting Chairperson Duane M. DesParte; PCAOB Staff; FINRA Staff Event: Small Business and Broker-Dealer Auditor Forum

Number 6 (Page 21)

EIOPA welcomes Solvency II proposals from the European Commission on sustainability

Number 7 (Page 23)

Driving different decisions today: putting climate scenarios into action

Sarah Breeden, at the MIT Golub Center for Finance and Policy 8th Annual Conference

Number 8 (Page 25)

NIST Draft Publication Addresses Removing Barriers for Voters With Disabilities

Number 9 (Page 28)

EU National Telecom Authorities analyse Security Supervision and Latest Security Threats

The EU National Telecom Authorities met in Athens, Greece for the 35th meeting of the ECASEC group. The European Union Agency for Cybersecurity also hosted the 1st Telecom Security Forum on this occasion.

Number 10 (Page 33)

DARPA Moving SSITH Safeguards Closer to Practical Use

Researchers to develop ASIC hardware with novel protections proven in the SSITH program, mitigating against software attacks on hardware

Number 1

Cybersecurity in 2022 Commission Work Programme

The European Commission has adopted its 2022 Work Programme, setting out the next steps in its bold and transformative agenda towards a post-COVID-19 Europe that is greener, fairer, more digital and more resilient.

This Commission Work Programme contains *42 new policy initiatives* across all six headline ambitions of President von der Leyen's Political Guidelines, building on her 2021 State of the Union speech.

It also reflects the lessons learnt from the unprecedented crisis caused by the pandemic, while paying particular attention to our young generation thanks to the proposed European Year of Youth 2022.

Cybersecurity has been mentioned especially in relation to one of six headline ambitions of President von der Leyen's Political Guidelines: 'A Europe fit for the digital age'. You may visit: https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_en.pdf

Among others, the Commission will propose a European Cyber Resilience Act to establish common cybersecurity standards, and begin building an EU space-based global secure communications system to provide additional EU-wide broadband connectivity and secure independent communications to Member States.

Moreover, as the energy sector will be the biggest contributor in meeting the EU's climate target of reducing emissions by at least 55 percent by 2030, the Commission will propose an action plan for an accelerated digital transformation of the sector, taking into account the need for resilient and cyber-secure energy.

Cybersecurity is also crucial if it comes to 'Promoting our European way of life'. The continued work on cybersecurity remains a crucial building block of the Security Union.

A Europe fit for the digital age

The pandemic has served as a catalyst for the accelerating digitalisation of Europe and the world. The Commission will follow up on its path to the digital decade to deliver on the EU's digital transformation by 2030.

We are determined to lead the way in the global race for trustworthy, secure and human-centric technology. And we will work to reach agreement on and implement our proposals for a safe and secure internet, a European digital identity and on trustworthy Artificial Intelligence.

The single market remains at the core of an innovative, prosperous and future-oriented European economy. Strong and effective competition policy and enforcement are needed to contribute to a resilient recovery and the twin transitions.

Against this background, the Commission has launched a review of competition policy to ensure that the various instruments are fit for purpose. We will also come forward with a single market emergency instrument to help prevent future disruptions.

Despite many challenges and disruptions, Europe came through the crisis in large part due to its innovative skills, its strong industrial base and its diversified and competitive supply chains. However, in a few strategic sectors, it has been vulnerable due to high dependency on a very limited number of non-EU suppliers, especially in relation to raw materials.

This is particularly apparent when it comes to semi-conductors. Supplies of these chips which power Europe's digital solutions have become a real concern for EU industry, with cases of production being slowed down.

Against this background, we will adopt a European chips act to promote a state-of-the-art European chip ecosystem to boost our innovative capacity, security of supply and develop new markets for ground-breaking European tech.

With the economy and society relying more and more on digital solutions, we need to ensure that we can defend ourselves in a world increasingly prone to hacking of connected products and associated services.

To this end, we will propose a European cyber resilience act to

establish common cybersecurity standards for products. We will also begin building an EU space-based global secure communications system, offering EU-wide broadband connectivity where it currently does not exist and secure and independent communications to Member States.

As the energy sector will be the biggest contributor in meeting the EU's climate target of reducing emissions by at least 55 percent by 2030, the Commission will propose an action plan for an accelerated digital transformation of the sector, which is needed to ensure the shift towards renewables, connected mobility, smart buildings, and a more integrated energy system with consumers at its core.

The wide-scale energy disruptions in the US and the EU over the past year show the need for resilient and cyber-secure energy.

For European citizens to benefit to the full from digital technology, the provision of strong digital skills and education is key. This was highlighted as distance learning became the norm during the COVID-19 pandemic. And it is highlighted as a key target in the Digital Compass.

To address the skills and knowledge gaps, we will propose measures to facilitate and promote digital skills in schools and higher education.

Research and innovation will play a key role in responding to the challenges facing us today. It will help deliver on Europe's recovery, based on economic growth that can drive the green and digital transitions.

This will be essential for fair economic growth benefiting all regions and citizens, including rural areas. It is important to ensure that Europe remains at the frontier of science and at the forefront of new waves of innovation.

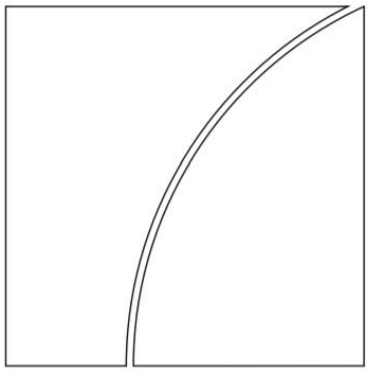
Digital solutions can also help support more integrated and sustainable mobility. We will propose an initiative on multimodal digital mobility services to address market gaps in the combined use of transport modes, including rail.

You may visit:
https://ec.europa.eu/info/sites/default/files/com2021_645_en.pdf

Number 2

Big techs in finance: on the new nexus between data privacy and competition

BIS



BIS Working Papers
No 970

Big techs in finance: on the new nexus between data privacy and competition

by Frederic Boissay, Torsten Ehlers, Leonardo Gambacorta and Hyun Song Shin

Monetary and Economic Department

October 2021

Focus

Large technology companies such as Alibaba, Amazon, Facebook, Google and Tencent have started to provide financial services. The activities of big techs in finance are a special case of broader fintech innovation.

While fintech companies are set up to operate primarily in financial services, big tech firms offer financial services as part of a much wider set of activities. Big techs' foray into finance raises both opportunities and risks.

Contribution

The contribution of this paper is threefold.

First, it describes big techs' business models and analyses the potential benefits in their provision of financial services such as financial inclusion and reduced asymmetric information problems in the supply of credit.

Second, it evaluates the potential costs, including the new risks of price discrimination, abuse of market power, anti-competitive behaviour and limits to data privacy.

Third, it lays out the complex public policy trade-off between the objectives of efficiency and privacy, and discusses the policy options

Findings

Big techs' entry in finance builds on their established digital platforms in e-commerce, search and social media, and holds the prospect of efficiency gains and greater financial inclusion.

Their business model rests on enabling direct interactions among a large number of users.

An essential by-product of their business is their large stock of user data, which are used as an input for a range of services that exploit natural network effects, generating further user activity.

Increased user activity then completes the circle, as it generates yet more data.

The self-reinforcing loop between data, network externalities and activities, is the DNA of big techs.

Big techs have the potential to become dominant through the advantages afforded by the data-network-activities DNA loop – raising competition and data privacy issues.

How to define and regulate the use of data has become an important policy issue for authorities and increases the need to coordinate policies at both the domestic and international level.

Abstract

The business model of big techs rests on enabling direct interactions among a large number of users on digital platforms, such as in e-commerce, search and social media.

An essential by-product is their large stock of user data, which they use to offer a wide range of services and exploit natural network effects, generating further user activity.

Increased user activity completes the circle, as it generates yet more data.

Building on the self-reinforcing nature of the data- network-activities loop, some big techs have ventured into financial services, including payments, money management, insurance and lending.

The entry of big techs into finance promises efficiency gains and greater financial inclusion.

At the same time, it introduces new risks associated with market power and data privacy.

The nature of the new trade-off between efficiency and privacy will depend on societal preferences, and will vary across jurisdictions.

This increases the need to coordinate policies both at the domestic and international level.

You may visit: https://www.bis.org/publ/work970.pdf

Number 3

FSB Chair's letter to G20 Finance Ministers and Central Bank Governors

This letter from the FSB Chair, Randal K. Quarles, to G20 Finance Ministers and Central Bank Governors ahead of their meeting on 13 October focuses on two key areas of the FSB's work on which the FSB has submitted reports to the upcoming G20 meeting:

Developing a more resilient NBFI sector

The letter notes that, following the market turmoil in March 2020, the FSB agreed on an ambitious multi-year workplan to enhance NBFI resilience.

A key priority of this workplan has been work to address vulnerabilities in money market funds (MMFs), conducted in collaboration with the International Organization of Securities Commission (IOSCO). The FSB has delivered to the G20 a final report with policy proposals to enhance money market fund resilience.

Table of Contents

Executive summary 1
1. Introduction 4
2. Forms, functions and roles of MMFs 6
   2.1. MMF types 6
   2.2. MMFs in the broader short-term funding ecosystem 8
   2.3. MMF functions for investors and borrowers 13
   2.4. Potential substitutes for MMFs 14
3. Vulnerabilities in MMFs 16
   3.1. Crisis experience and policy responses 16
   3.2. Types of vulnerabilities in MMFs 20
4. Policy proposals to enhance MMF resilience 22
   4.1. Categorising policy options 22
   4.2. Assessing potential substitutes for MMFs 23
   4.3. Assessment of policy options 26

5. Adopting complementary measures on risk monitoring and short-term funding markets 37
6. Considerations in selecting policies 39
6.1. Prioritising MMF policy options 39
6.2. Combining MMF policy options 40
Annex A: MMFs and short-term funding markets 43
Annex B: Assessment framework 47
Annex C: Assessment of variants of MMF policy options 49
Annex D: Glossary of terms 59
Abbreviations 61

You may visit:
https://www.fsb.org/2021/10/policy-proposals-to-enhance-money-market-fund-resilience-final-report/

FSB members are assessing, or will assess, MMF vulnerabilities in their jurisdiction and will address them using the framework and policy toolkit in the report, in line with their domestic legal frameworks.

The FSB, working with IOSCO, will then take stock of progress made and assess the effectiveness of the measures taken. The FSB and IOSCO will also carry out further work, complementing MMF policy reforms, to enhance the functioning and resilience of short-term funding markets.

The letter also notes the considerable progress made on assessing vulnerabilities and identifying policy considerations in other areas within NBFI, including open-ended funds; the impact of margin calls; and the structure of core funding markets.

The FSB will leverage insights from the analysis in these areas to develop a systemic risk perspective on NBFI and policies to address such risks. The FSB will submit to G20 Leaders later this month a full progress report on its work to enhance resilience of NBFI, including areas where continued focus is needed.

Addressing challenges in cross-border payments

The COVID Event has brought into even sharper focus the need to address the limitations of current arrangements for cross-border payments.

Last year, the FSB delivered a roadmap to enhance cross-border payments, so they are faster, more inclusive, less expensive and more transparent.

Taking forward work on the roadmap, the FSB is submitting to the G20:

- a progress report on the roadmap to enhance cross-border payments, which also confirms steps for next year and beyond;

- quantitative targets for addressing the challenges of cost, speed, transparency and access experienced by end-users; and

- a report on the progress made on the implementation of the FSB's high-level recommendation for the regulation, supervision and oversight of "global stablecoin" arrangements.

The letter notes that the FSB will also be submitting its latest work on cyber incident reporting, which brings together cross-sectoral expertise to explore whether harmonisation in cyber reporting can be achieved and what additional work needs to be undertaken.

To read more: https://www.fsb.org/wp-content/uploads/P111021-1.pdf

Number 4

How Long is Too Long? How High is Too High?: Managing Recent Inflation Developments within the FOMC's Monetary Policy Framework

Governor Randal K. Quarles, at the 2021 Milken Institute Global Conference "Charting a New Course," Beverly Hills, California

Thank you to the Milken Institute for the opportunity to join you today. This morning I'd like to outline my view of current economic conditions and the economic outlook and then turn to the implications for monetary policy.

In particular, with employment still well below its February 2020 peak, I will focus on how the escalation in inflation this year is testing the monetary policy framework adopted by the Federal Open Market Committee (FOMC) in August 2020.

Outlook for Economic Growth

Recent data suggest that growth in the third quarter is likely to be lower than we had expected, but the foundations remain in place for strong economic growth over the remainder of this year and next.

Employment is growing, financial conditions are accommodative, businesses are investing, and households, in the aggregate, have a large stock of savings to draw on for future spending.

Weaker growth in payrolls in August and September, along with uneven consumer spending in July and August, appear to reflect ongoing concerns in some parts of the country about the spread of COVID-19, especially in high-contact service industries.

Supply bottlenecks and labor shortages that have been more widespread and persistent than many expected are camouflaging continued strong underlying demand for goods, services, and workers.

Supply constraints are particularly evident in interest-sensitive parts of the economy, such as residential investment and vehicle sales, limiting the scope for additional monetary accommodation to stimulate activity in those sectors.

I expect that these developments, however, have for the most part simply postponed activity temporarily and that robust growth will return in the coming months. There is evidence in recent weeks that we seem to be moving into a new phase of the economy.

Nominal retail sales rose seven-tenths of 1 percent in September on the heels of a nine-tenths increase in August, an indication that consumers kept up their pace of spending.

Robust business investment in equipment and intangibles continued in the second quarter, and indicators suggest another gain in the third quarter. Forward indicators of business spending and the need for firms to replenish depleted inventories point to strong investment into next year.

The Labor Market Continues to Strengthen

Without a doubt, the headline job gains in August and September were lower than expected, but, as I will show, based on almost every other major labor market indicator, there is ample evidence that the demand for labor is strong.

At last measure, the Labor Department reported that job openings remained near a record high in August, and a record number of workers were voluntarily quitting their jobs, an indicator of their confidence in finding a better one.

Other measures of job openings by education level indicate that jobs are plentiful even for less-skilled workers who have been affected the most by the COVID event.

Another indicator I've been watching closely is the so-called U-6 unemployment rate, which consists of people who are working part time but prefer full-time work and discouraged workers who want a job but have given up looking.

U-6 unemployment declined significantly over the past two months to 8.5 percent in September, roughly the same level as in the middle of 2017, when most everyone considered the job market to be quite healthy.

In fact—and this will not be news to most of you—shortages of skilled workers in many occupations predated the COVID event and are likely to persist after its effects have faded.

Some of this shortage reflects the aging of the workforce, changes in the types of jobs people want to do, and the time it takes to train workers.

Strong demand for labor is outpacing supply, and, naturally, that development is putting upward pressure on wages. Through September, average hourly wages are up 4.6 percent over the past 12 months, the largest and most sustained increase in wages for workers since the 1990s.

I noted the imbalance between the demand and supply for labor, and some of the labor market indicators that are still well short of pre-COVID levels are those related to labor force participation, which has been about unchanged this year on balance.

I expect that as conditions normalize, this measure will pick up, but it is unlikely to return to its February 2020 level.

One reason is that a disproportionate number of older workers responded to the initial shock of the COVID event by retiring, which may be an area where participation and employment struggle to retrace lost ground.

Longer-lasting changes in labor force participation could make wage pressures more persistent and have implications for the assessment of maximum employment.

Tapering Asset Purchases

Since the middle of last year, the Fed has been increasing its holdings of Treasury securities and agency mortgage-backed securities by $120 billion a month to foster smooth market functioning and to support the economy by putting downward pressure on interest rates.

Conditions had improved considerably by the time we announced our forward guidance for asset purchases in December, but the unemployment rate remained at 6.7 percent, near-term growth was being constrained by heightened social-distancing restrictions amid surging hospitalizations from COVID-19, and inflation was running significantly below 2 percent.

As we sit here today, demand for labor is strong, and unemployment has declined to 4.8 percent. We have exceeded the previous high for real gross domestic product and are close to reaching the pre-COVID trend. Inflation, about which I will say more shortly, is running at more than twice the FOMC's longer-run goal.

Taking all of the evidence into account, I think it is clear that we have met the test of substantial further progress toward both our employment and our inflation mandates, and I would support a decision at our November meeting to start reducing these purchases and complete that process by the middle of next year.

Bear in mind that asset purchases are pressing down on the accelerator, adding each month to the amount of accommodation the Fed is providing to the economy through downward pressure on longer-term interest rates. Reducing purchases and ending them on this schedule is not monetary tightening, but a gradual reduction in the pace at which we are adding accommodation.

To read more:
https://www.federalreserve.gov/newsevents/speech/quarles20211020a.htm

Number 5

Forum for Auditors of Small Businesses and Broker-Dealers

PCAOB Acting Chairperson Duane M. DesParte; PCAOB Staff;
FINRA Staff Event: Small Business and Broker-Dealer Auditor Forum

In September 2021, the PCAOB announced that its Forum for Auditors of Small Businesses and Broker-Dealers would not take place in person in 2021 due to the COVID-19 pandemic.

The following resources are offered in place of the in-person Forum.

Video: https://www.youtube.com/watch?v=QoxNj8ZOOuY

Video: https://www.youtube.com/watch?v=y1-PLGDV46A

The slides:
https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/news/events/documents/10202021--forum-for-auditors-of-small-businesses-and-broker-dealers/final--2021-oca-presentation.pdf?sfvrsn=f56e0e0_3

Video: https://www.youtube.com/watch?v=K_CDsNSFhgM

The slides:
https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/news/events/documents/10202021--forum-for-auditors-of-small-businesses-and-broker-dealers/final--2021-dei-presentation.pdf?sfvrsn=c49aa5db_3

Video: https://www.youtube.com/watch?v=JohieGTAdMk

The slides:
https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/news/events/documents/10202021--forum-for-auditors-of-small-businesses-and-broker-dealers/final--dri-(issuer)-update.pdf?sfvrsn=736ea1ca_3

Video: https://www.youtube.com/watch?v=oX7P3hSmW1k

The slides:
https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/news/events/documents/10202021--forum-for-auditors-of-small-businesses-and-broker-dealers/final--2021-dri-(issuer)-illustrative-examples.pdf?sfvrsn=5c7f41e6_4

To read more:
https://pcaobus.org/news-events/events/event-details/2021-forum-for-auditors-of-small-businesses-and-broker-dealers

Number 6

EIOPA welcomes Solvency II proposals from the European Commission on sustainability

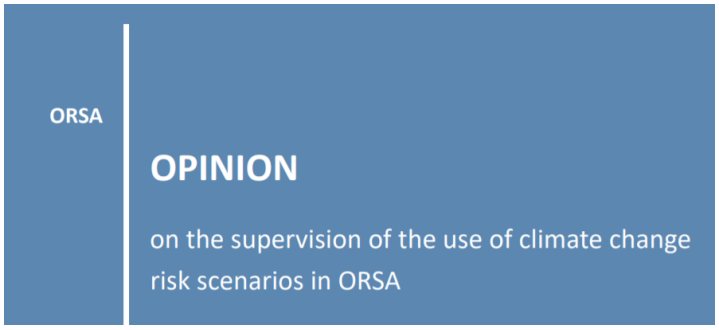
The European Insurance and Occupational Pensions Authority (EIOPA) welcomes the Solvency II proposals of the European Commission to give mandates to EIOPA for further action on sustainable finance.

EIOPA is convinced that these proposals would contribute positively to a transition into a more sustainable economy and that insurers, in their role as investors and risk managers, can facilitate it.

In particular, EIOPA welcomes the two mandates proposed by the European Commission regarding sustainability risks. EIOPA believes that it is important to explore prudential treatment of exposures related to assets or activities associated substantially with environmental or social objectives.

Furthermore, a regular review of the scope and the calibration of parameters of the standard formula pertaining to natural catastrophe risk is an important step towards a more sustainable framework.

EIOPA is also pleased about the inclusion of climate change scenarios in the Own Risk and Solvency Assessment (ORSA), which reflects EIOPA's opinion earlier in 2021. The opinion: https://www.eiopa.europa.eu/media/news/eiopa-issues-opinion-supervision-of-use-of-climate-change-risk-scenarios-orsa_en



EIOPA considers it essential to foster a forward-looking management of climate change-related physical and transition risks to ensure the long-term solvency and viability of the industry.

To read more:
https://ec.europa.eu/info/publications/210922-solvency-2-communication_en

https://www.eiopa.europa.eu/media/news/eiopa-welcomes-solvency-ii-proposals-european-commission-sustainability_en

Number 7

Driving different decisions today: putting climate scenarios into action

Sarah Breeden, at the MIT Golub Center for Finance and Policy 8th Annual Conference

Sarah Breeden speaks about the system-wide and economy-wide impacts of climate change, using insights from the most recent work we have led through the central banks and supervisors Network for Greening the Financial System (NGFS) on climate scenarios.

She shares lessons we have learned from designing and applying climate scenarios, as well as some thoughts on their future, including the vital contribution research needs to make.

Introduction

We are now only 11 days away from COP26 in Glasgow.

Climate science tells us that the planet has already warmed by about 1.1 degree Celsius since pre-industrial times.

Indeed, the news is full of the devastating effects of physical changes already taking place around us. And existing commitments from countries to reduce greenhouse gas emissions are not enough to keep warming to well below 2 degrees, let alone 1.5.

The United Nations Intergovernmental Panel on Climate Change (IPCC) estimates we will reach 1.5 degrees by 2040 even under their 'very low emissions' scenario.

Failure to formulate more ambitious commitments and deliver against them this decade will mean we miss the last opportunity significantly to deter the course of climate change.

The case for action is clear - the question is whether our actions will match that case, in particular whether we turn aspiration into action on the scale required. Delivering a path to net zero requires all of us to take necessary steps – governments and business, investors and individuals, as well as central banks and financial regulators.

Here at the Bank of England, we have taken a range of actions in line with our objectives – including setting expectations for banks and insurance companies on their approaches to managing climate-related financial risks, running a system wide climate scenario exercise, and setting out how to green our corporate bond purchase scheme – to play our part in the transition to a net zero economy.

Through all this work, one thing has become abundantly clear – that the actions we take today will determine the consequences we face in the years to come. And so if we are to take the right decisions, we must stretch our horizons, taking different decisions today well before the consequences of inaction manifest at scale.

This needs to occur across the entire economy. And the financial system needs to be a key enabler. As central bank and financial regulator, these implications put climate change squarely within our remit.

We cannot solve climate change and drive the transition – those with the responsibility and tools to do this sit elsewhere in government and industry. But we must ensure that the financial system is resilient to climate-related financial risks, that it can support the transition, and that we understand its macroeconomic impacts.

Today, I want to speak specifically on the system-wide and economy-wide impacts of climate change, using insights from the most recent work we have done on climate scenarios through the central banks and supervisors Network for Greening the Financial System (NGFS).

I will cover three things: first, lessons we've learned from designing climate scenarios; second, lessons we've learned from applying them; and third, I will share some thoughts on the future of scenario analysis – including the vital contribution research needs to make.

To read more:
https://www.bankofengland.co.uk/speech/2021/october/sarah-breeden-keynote-presentation-at-the-mit

Number 8

NIST Draft Publication Addresses Removing Barriers for Voters With Disabilities

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

As part of the federal government's effort to improve access to voting, the National Institute of Standards and Technology (NIST) has released a draft publication outlining barriers that voters with disabilities may encounter during the election process — as well as potential approaches for addressing them. NIST is requesting comments on the draft by Nov. 22, 2021, to inform a final version expected in December.

The draft publication, formally titled Promoting Access to Voting: Recommendations for Addressing Barriers to Private and Independent Voting for People with Disabilities (NIST Special Publication 1273), forms part of NIST's response to the March 7, 2021, Executive Order (EO) 14019 on Promoting Access to Voting. You may visit: https://www.nist.gov/system/files/documents/2021/10/21/Report%20Draft%20EO%20Promoting%20Access%20to%20Voting_FRN-508-v2.pdf

Draft NIST Special Publication 1273-draft

Promoting Access to Voting: Recommendations for Addressing Barriers to Private and Independent Voting for People with Disabilities

The draft reflects the 171 public comments NIST received to its Request for Information (RFI) of June 2021 on barriers that people with disabilities encounter at all stages of the election process.

"The majority of the responses we received to the RFI were from individuals with disabilities," said NIST's Sharon Laskowski, an author of the draft. "Some responses were from advocacy groups, and a few more came from vendors and from state and local election officials, but we were pleased to see the number of individuals who took the time to respond."

Some of the comments from individuals are highlighted in the draft publication text as blue-tinted "quote bubbles" that describe personal experiences of barriers to voting. One response from a voter who uses a

wheelchair describes a precinct that in 2021 remains inaccessible, while another from a person with low vision indicates that poll workers often do not know how to turn on the voice feature in voting machines — in this case needing two hours to figure out how.

“People spoke from the heart, and they expressed how important it was for them to be able to vote independently and privately,” Laskowski said. “The comments we received ranged across all 20 topics we listed in the RFI.”

The draft publication is organized into seven chapters: an introduction followed by six others dedicated to parts of the voting process. Each chapter that follows the introduction presents a class of barriers followed by potential means of addressing them.

Chapter 2 concerns systemic barriers that people with disabilities may encounter across the voting process. For instance, voters who rely on alternative communication, language and interaction styles face barriers when searching for information, whether by requesting election information on paper, asking for it in person or registering to vote online.

Chapters 3 to 7 each concern a specific part of the voting process mentioned by name in Section 7 of the EO, including barriers encountered at polling places or when interacting with voting technology.

Chapter 3, in particular, concerns the online Federal Voter Registration Form, which the EO indicates could be accessible to all voters, but which in its current form may present obstacles that cause voters with disabilities to use it far less frequently.

For example, the form must be physically signed and returned, which is a challenge for voters who have difficulties reading printed text or handling paper.

While the draft makes general recommendations concerning these barriers — such as improving poll worker training and making polling locations more accessible — the authors do not make suggestions for how any specific voting jurisdiction should implement them, given the many differences among the nation’s jurisdictions, which number in the thousands.

“We want to see these recommendations implemented so that voting systems are accessible to all voters, but we also recognize that jurisdictions will have to consider their own unique circumstances when removing barriers,” Laskowski said. “This NIST publication aims to help state and local officials analyze situations in their own context and improve accessibility for their own voters with disabilities.”

NIST will accept comments on the draft document until Nov. 22, 2021. Commenters are encouraged but not required to use the comment template. Comments may be submitted by email to pva-eo@list.nist.gov or at www.regulations.gov. For complete instructions for submitting comments, go to the Federal Register notice or NIST's voting webpage.

The draft report is available for review online at: https://www.nist.gov/system/files/documents/2021/10/21/Report%20Draft%20EO%20Promoting%20Access%20to%20Voting_FRN-508-v2.pdf

Number 9

EU National Telecom Authorities analyse Security Supervision and Latest Security Threats

The EU National Telecom Authorities met in Athens, Greece for the 35th meeting of the ECASEC group. The European Union Agency for Cybersecurity also hosted the 1st Telecom Security Forum on this occasion.

Launched more than 10 years ago, the European Competent Authorities for Secure Electronic Communications (ECASEC) group serves as a platform for collaboration and exchange of information among the national authorities supervising telecom security in Europe.

The ECASEC group also develops and endorses guidelines for telecom security authorities on how to implement different aspects of EU telecom security policy.

Besides the ECASEC meeting, the EU Agency for Cybersecurity (ENISA) hosted the 1st edition of the ENISA Telecom Security Forum on 13 October.

The goal of this event, held in a hybrid format, was to bring together experts from both national authorities and the private sector to exchange views and discuss cybersecurity challenges and good practices.

Highlights of the 35th ECASEC Expert Group meeting

A total of more than 50 experts from national authorities supervising the European telecom sector in the EU, EFTA, EEA, and EU candidate countries attended the meeting held on 14th October, with almost a third of them being present physically.

The meeting was the opportunity for the experts to follow an analysis of the supply chain threat landscape recently published by ENISA. BEREC also presented their report on the location of the Network Termination Points.

The location of the Network Termination Points has an impact on whether an equipment is part of the public network or part of the telecommunications terminal equipment (TTE) and that distinction affects in turn the legal power of the National Regulatory Agencies (NRAs).

ENISA introduced the main points of the upcoming ENISA reports on Consumer Outreach and Network Function Virtualisation (NFV) Security

and participants listened to an analysis of Confidentiality, Integrity and Authenticity attacks in public electronic communication networks.

This type of attacks is of great interest for the members of the ECASEC Expert Group since the definition of security in the EECC includes also confidentiality of communications.

Finally, the group dived into the recent Facebook outage and stressed the need for streamlining the incident reporting process so as to avoid unclear and overlapping obligations on providers and effectively cover cross-border incidents that involve several countries.

The 1st edition of the ENISA telecom security forum in a nutshell

A total of more than 250 telecom security experts met both physically in Athens and online to discuss the following points of the agenda:

- latest developments on the Electronic Communications Framework and other legislative initiatives at both European and national levels;

- good practices and experience in dealing with emerging security threats;

- emerging technologies and related initiatives.

The Forum was opened by Evangelos Ouzounis, Head of the Policy Development and Implementation Unit of ENISA and by Warna Muzenbrock, chair of the ECASEC group.

They both highlighted the challenges and opportunities of the new regulatory environment for the telecom sector.

On behalf of the Greek mobile operators, George Stefanopoulos welcomed the participants and highlighted the challenges for operators during the pandemic and in view of the 5G rollout.

The forum had three parts: a policy session about EU legislation, a technical session about ongoing cyber threats and a future networks session, with talks including topics such as 5G and edge computing.

The Policy session:

The Forum focused on the latest policy developments, the European Electronic Communications Code (EECC) and the updated NIS Directive (NIS2) and how these affect the European telecom operators.

The policy session started with an intervention from the European Commission presenting the NIS2 proposal and its implications for the telecom sector.

Magnus Falk from ZOOM and Paolo Grassia from the European Telecommunications Network Association analysed the impact of the new legislation on telecom providers, both Number-Independent Interpersonal Communication Services providers and traditional ones.

Finally, Kinga Pawlowska from a Polish media law firm discussed recent legislative proposals in Poland addressing the EECC and the NIS Directive.

The Analysis of current threats and attacks – Technical session:

The technical session of the Forum included a presentation of the sub-sea fibre network of Liberty Global and an analysis of SIM Swapping attacks by Europol. Additionally, the Centre for Cybersecurity of Denmark shared their work on the threat from ransomware for the telecoms sector.

Kevin Meynell, from the Internet Society, explained the MANRS project, an industry collaboration that aims to set good practices for more secure Border Gateway Protocol (BGP) routing.

The future networks session:

Julie Ruff, Deputy Head of Unit of Cybersecurity Technologies and Capacity building of European Commission DG CNECT, introduced the work of the 5G cybersecurity work stream of the NIS Cooperation Group. Silke Holtmanns, from Adaptive Mobile Security, member of the ENISA Advisory Group, presented an analysis of the Secure Integration of 5G Private Networks.

The discussions focused on threat vectors seen in Multi Edge Computing (MEC) deployments and the security controls deployed by service providers. GSMA presented its Network Equipment Security Assurance Scheme (NESAS).

The presentations:
https://www.enisa.europa.eu/events/enisa-telecom-security-forum/telecom-security-forum-agenda

You may visit:
https://www.enisa.europa.eu/events/enisa-telecom-security-forum/etsf-presentations/sim-swapping-enisa.pdf

You may visit:
https://www.enisa.europa.eu/events/enisa-telecom-security-forum/etsf-presentations/enisa-briefing-about-ransomware-threat-13-okt-2021_without-notes.pdf

The bridge to possible

Securing your 5G infrastructure to the edge and beyond

For ENISA

Pramod Nair
Security - Cisco
13 Oct 2021

You may visit:
https://www.enisa.europa.eu/events/enisa-telecom-security-forum/etsf-presentations/enisa_presso.pdf

Number 10

DARPA Moving SSITH Safeguards Closer to Practical Use

Researchers to develop ASIC hardware with novel protections proven in the SSITH program, mitigating against software attacks on hardware

DARPA's System Security Integration Through Hardware and firmware (SSITH) program is exploring hardware security architectures and tools that protect electronic systems against common classes of hardware vulnerabilities exploited through software, with the goal of breaking the endless cycle of software patch-and-pray.

To date, research on the program has focused on developing approaches and proving out concept that system-on-chip (SoC) designers can use to limit computer hardware to states that are secure while maintaining performance and power.

After rigorous testing and evaluation, researchers have proven that SSITH concepts provide robust hardware safeguards against known common weakness enumeration (CWE) classes of hardware vulnerabilities.

The SSITH program is now entering a final stage and is focused on transitioning and converting the proven concepts from lab discoveries to practical application.

The team from Lockheed Martin Corporation is moving beyond virtual processors and aims to develop an application-specific integrated circuit (ASIC) that integrates a dual-core Arm processor and multiple peripheral interfaces with embedded security capabilities provided by their proven SSITH approach, known as Hardware Architecture Resilience by Design (HARD).

Lockheed Martin's HARD utilizes an approach to provide a hardware solution to protect systems against multiple classes of hardware vulnerabilities.

Rather than perform "major surgery" on the CPU pipeline in order to implement new instructions or change the format of a pointer, the HARD approach utilizes a set of pipelines running in parallel to the primary CPU execution pathway to act as a parallel security co-processor, monitoring the main CPU and standing ready to flag any malicious operations.

Each pipeline monitors the stream of instructions executing on the main CPU pipeline, deriving the current semantic context based on expected patterns of instructions, and looking for any exploitation attempts.

HARD pipelines can be aggregated to deploy more or less security coverage as needed for the target environment, essentially enabling a user to only pay for what they need. In addition, because there is no need for major modifications to the primary CPU, HARD can be deployed to enforce security across any CPU architecture.

“By bringing HARD protections to an ASIC, we’re bringing SSITH technology one step closer to practical use,” said Keith Rebello, the program manager leading SSITH. “Lockheed Martin expects to spend the next two years transitioning HARD from the laboratory to a secure processor that we can integrate with other computing hardware, ultimately demonstrating SSITH’s ability to protect real-world systems from exploitation.”

To read more: https://www.darpa.mil/program/ssith

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.

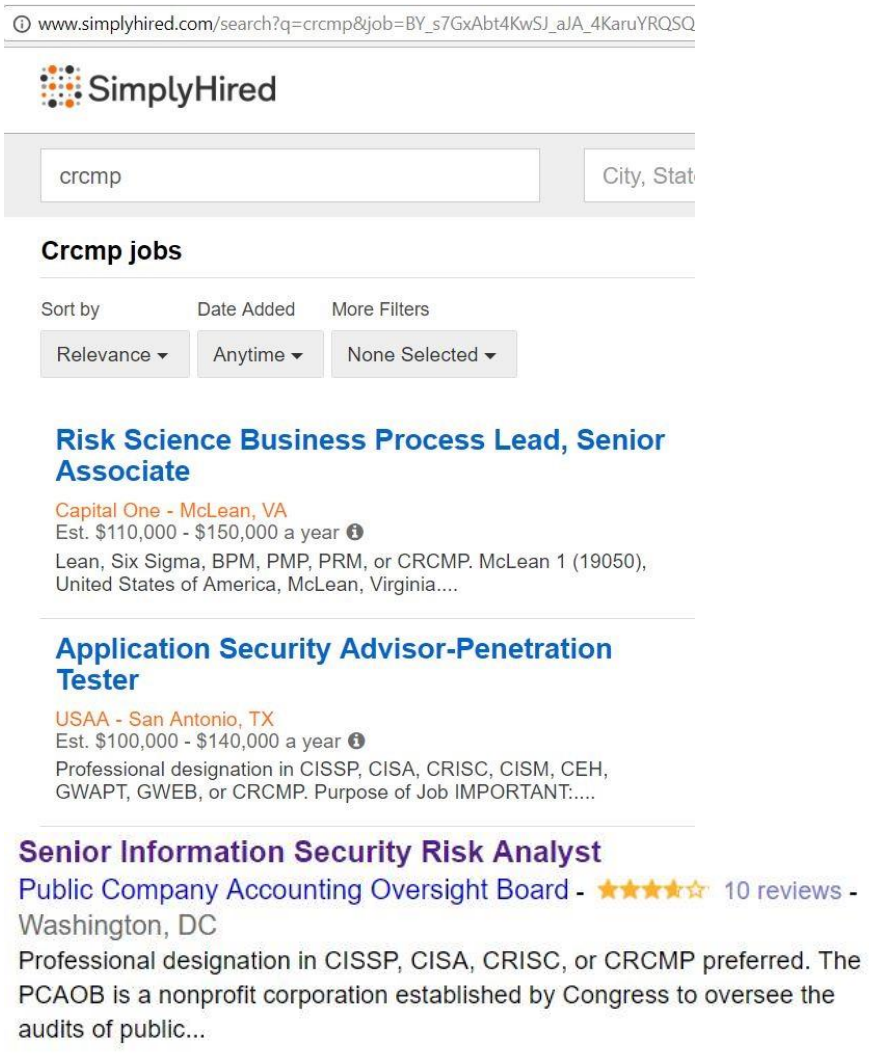
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

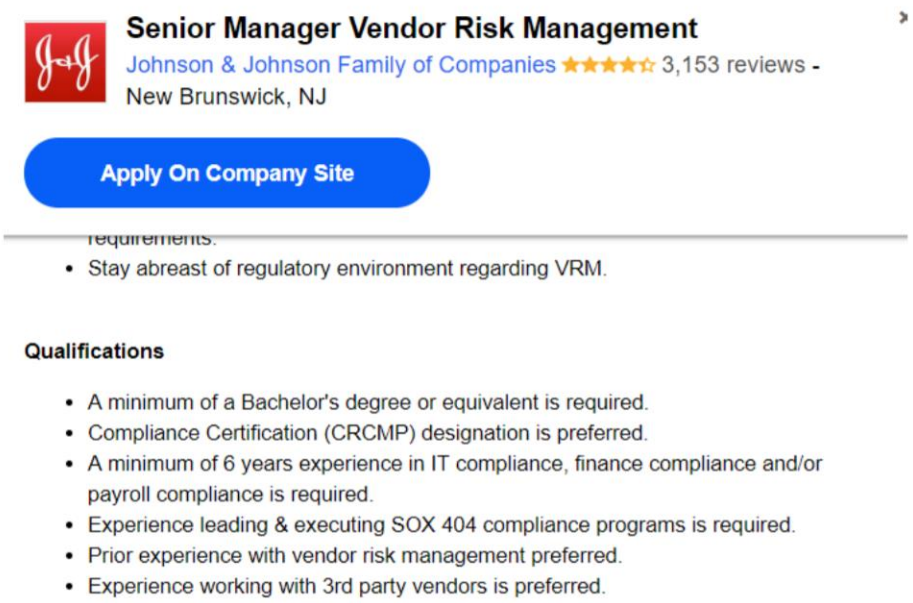
You can explore what we offer to our members:

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.