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

Monday, July 4, 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,

During the weekend, I read for the second time the *2021 Annual Report* from the European Banking Authority (EBA). This is a very interesting document, especially for those than need to know where we are, and what is next.

I did not start from the first page. I was very interested in the legislative proposals for a regulation on *markets in crypto-assets (MiCA)* and the regulation on *digital operational resilience for the financial sector (DORA).*

In 2021 the Joint Committee stepped up its digital-finance-related work, with extensive technical discussions on topics such as crypto-assets and digital operational resilience. In addition, the European Supervisory Authorities (ESAs) prepared a comprehensive response to the European Commission's February 2021 call for advice on digital finance regarding

value chains, platformisation and new mixed activity groups.

Most notably, the report envisaged possible ways to foster the regulation and supervision of mixed activity groups, among others by enhancing cooperation between financial and other relevant authorities, and potentially by expanding and strengthening the perimeter of consolidation.

We can also read that the EBA expects to receive a specific request from the European Commission to explore the extent to which the EU Taxonomy could be applied to identify *green retail products*. As part of this work, the EBA will assess current market practices and will identify potential impediments to the scaling up of *green lending* to retail customers in the EU. It will also investigate how to ensure appropriate monitoring of the use of proceeds of green loans and avoid the risk of *'greenwashing'*.

One of the priorities for the EBA in 2022 will be to discuss how to best include *climate risk* in a *stress test framework* in light of the proposed mandates outlined by the European Commission in its renewed strategy on sustainable finance published in 2021 and then translated into the draft CRD VI text. The strategy includes mandates for the EBA to issue guidelines for banks and supervisors on *ESG stress testing*.

The EBA is also looking to further enhance market discipline and promote the use of *Pillar 3* information facilitating centralised access by becoming a hub of Pillar 3 disclosures for EEA credit institutions. The Pillar 3 data hub aims to offer *easy access* to Pillar 3 information for all EEA institutions, facilitating cross-sector comparability of information and digitally user-friendly visualisation tools.

I found interesting the role of *environmental risks* in the *Pillar 1* framework. The EBA is mandated to assess whether a dedicated prudential treatment of exposures associated substantially with environmental objectives, or subject to environmental impacts, would be justified.

To address these mandates, covering both the framework for credit institutions and for investment firms, the EBA will be following a *two-step* approach.

In 2022 the EBA published a discussion paper, in which the analysis will be initiated and on which stakeholders will be invited to provide their feedback.

The feedback received on this discussion paper, together with available data and insights gained from the EU and international initiatives, will inform

the final report and related EBA policy recommendations, which should be finalised in 2023.

Read more at number 4 below. Welcome to the Top 10 list.

Best regards,

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

Number 6 (Page 25)

Botnet Disrupted in International Cyber Operation

THE UNITED STATES ATTORNEY'S OFFICE
SOUTHERN DISTRICT of CALIFORNIA

Number 7 (Page 28)

FBI Las Vegas Federal Fact Friday:
Social Media Money Flipping Scam

Number 8 (Page 30)

Miners as intermediaries: extractable value and market manipulation in crypto and DeFi
BIS Bulletin 58, Raphael Auer, Jon Frost and Jose María Vidal Pastor

BIS

Number 9 (Page 33)

NIST Releases Draft IR 8409
Measuring the Common Vulnerability Scoring System Base Score Equation

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

Number 10 (Page 35)

Voices from DARPA Podcast Episode 57
Unmasking Misinformation & Manipulation

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 1

The digital euro and the evolution of the financial system

Fabio Panetta, Member of the Executive Board of the European Central Bank, at the Committee on Economic and Monetary Affairs of the European Parliament, Brussels

I am pleased to join you here today to discuss the progress we have made in our digital euro project.

A digital euro would enable Europeans to use public money for digital payments throughout the euro area – just like they can use cash for physical payments.

Bringing central bank money into the digital era is a logical step as payments become increasingly digitalised. And this is critical for two main reasons.

First, we need to preserve the role of public money as the anchor of the payments system in order to ensure the smooth coexistence, the convertibility and the complementarity of the various forms that money takes. A strong anchor is needed to protect the singleness of money, monetary sovereignty and the integrity of the financial system.

Second, a digital euro would contribute to our strategic autonomy and economic efficiency by offering a European means of payment that could be used for any digital payment, would meet Europe's societal objectives and would be based on a European infrastructure.

We will design the digital euro in a way that makes it attractive to users, who would like to use it to pay anywhere.

Giving legal tender status to the digital euro would make this possible, and it will be decided by you, the co-legislators. It would also help to achieve the network effects that are key to the success of payment solutions.

We will also strive for the highest standards of privacy and aim to contribute to financial inclusion and foster digital innovation, including as regards the programmability of payments.

As for implementation, we are working to minimise the time to market, costs, risks and ecological footprint associated with the digital euro.

In particular, we will make sure that the digital euro builds on the experience of financial intermediaries in consumer-facing services, does not crowd out private means of payment, and preserves financial stability. And this is the aspect that I will focus on today: the potential impact of a digital euro on the financial system.

The digital euro and the evolution of the financial system

As we explore the design of the digital euro, we are not only looking at the payments landscape of today – we are in fact also considering how it might evolve in the future.

Imagine a world in which the central bank continues to offer only cash, but people increasingly prefer to pay digitally and the only digital forms of money available to them are private ones. In such a world, central bank money would lose its key role in payments, and it would not be possible to ensure the complementarity and convertibility of public and private money.

The entire monetary and financial sector would be deprived of its anchor – central bank money – and would be exposed to potential instability.

It is also conceivable that non-European digital payment solutions and technologies operated abroad might dominate our payments market, as we are already seeing in some segments like cards and online payments.

This risk would be exacerbated by the expansion of means of payment offered by big techs, which could use their very large customer base to their advantage.

This would raise questions about our autonomy and privacy in payments. It could even endanger European sovereignty.

Moreover, the international monetary system may see the emergence of central bank digital currencies (CBDCs) in large economies. Such CBDCs would offer benefits in terms of efficiency, scalability, liquidity and safety that would support their attractiveness internationally.

And they would have the potential to facilitate cross-border payments, which may enhance their role as a global payment unit. In such a context, not issuing a digital euro could undermine the international role of the euro and create additional risks to sovereignty.

This scenario is not imminent, but it could potentially materialise in the future if we do not start acting today. And if we don't act, we will also see increasing confusion about digital money. Crypto-assets are a case in point.

Unbacked crypto-assets, for example, cannot perform the functions of money. They are neither stable nor scalable. Transactions are slow and costly. And, in some forms, they pose a danger to the environment and to other societal objectives.

Stablecoins, meanwhile, are vulnerable to runs, as we have recently seen with algorithmic stablecoins. In this context, it is vital that any remaining regulatory gaps in the crypto-asset ecosystem are closed.

I count on the work of this Parliament to ensure that an ambitious regulatory framework emerges from the current negotiations on the EU Regulation on Markets in Crypto-Assets (MiCA) and on the current legislative proposals on anti-money laundering and countering the financing of terrorism, especially in relation to information accompanying transfers of funds and certain crypto-assets (FCTR).

To avoid this confusion about what digital money is and what it is not, we need the central bank to provide one of its own, responding to the demand for digitalisation and providing an anchor of stability in the world of digital finance.

Protecting the stability of the financial system

For the digital euro to play this role, we need to carefully evaluate its potential impact on monetary policy, financial stability and the provision of services by financial intermediaries.

A digital euro would of course be issued by the central bank. And unlike potentially dominant private actors in tomorrow's digital payments market – such as big techs – the central bank would pay close attention to financial stability considerations and to preserving a diverse and vibrant ecosystem.

This does not imply that the status quo must be maintained. It means that any potential risks emerging from the introduction of a digital euro should be contained in both normal times and times of financial stress. We have been discussing these aspects in detail over the past few months.

We are looking very closely at the risks to monetary policy transmission and financial stability that could be associated with the conversion of large parts of euro area bank deposits into digital euro.

Deposits represent the main source of funding for euro area banks today. If not well designed, a digital euro could lead to the substitution of an excessive amount of these deposits.

Banks can respond to these outflows, managing the trade-off between funding cost and liquidity risk.

The attractiveness of commercial bank deposits will also influence the degree of substitution.

But any undesirable consequences that may result from the issuance of digital euro for monetary policy, financial stability and the allocation of credit to the real economy should be minimised in advance by design.

And it is indeed possible to design a digital euro with effective tools to prevent it from being used as a form of investment rather than solely as a means of payment.

To read more: https://www.bis.org/review/r220616a.pdf

Number 2

Competitiveness and productive investment - what parts do they play in the reform of insurance regulation?

Ms Charlotte Gerken, Executive Director of Insurance Supervision of the Bank of England, at the JP Morgan European Insurance Conference.

Thank you for your introduction and for inviting me to this conference. Since the Government announced the **Solvency II review**, there has been much emphasis on the desirability of reform to enhance the insurance sector's competitiveness and its capacity to make productive investment.

Today I would like to outline how competitiveness and productive investment relate to the Prudential Regulation Authority's (PRA) approach to the review by focussing on three areas:

1. Investment flexibility
2. The valuation of liabilities
3. Process improvements

To put the review in context, though: the core framework underlying the Solvency II regime and its principles are broadly fit for purpose, and are in line with existing and emerging international standards.

The review does not involve tearing it up and starting again – not least because of the substantial sums invested by industry in the last decade in adopting it.

Industry responses to HM Treasury's Call for Evidence were largely in agreement with this approach.

However, the review does give an opportunity we are seizing, to deal with those areas of Solvency II that we know are not working as well as they could.

Sam Woods and I have both previously discussed the PRA's concerns relating to the current regime.

Taken together, the improvements we want to make represent an important set of reforms and can achieve the objectives of the review.

Objectives for the Solvency II review

The Government set three high level objectives for regulatory reforms, namely

1. to spur a vibrant, innovative, and internationally competitive insurance sector;

2. to protect policyholders and ensure the safety and soundness of firms; and

3. to support insurance firms to provide long-term capital to underpin growth, including investment in infrastructure, venture capital and growth equity, and other long-term productive assets, as well as investment consistent with the Government's climate change objective.

These Government objectives are aligned with the PRA's two primary statutory objectives of safety and soundness of regulated firms, and protection of policyholders.

The PRA's statutory objectives are reflected directly in one of the Government's review's objectives, and they underpin the other two: only a financially sound insurance sector can provide sustainable contributions to long-term investment.

Similarly, the sector's competitiveness depends on its operating under a robust prudential regime.

The first and third of the Government review objectives are also mutually supportive: breadth of investment is essential to the business model of a large part of the UK industry, so by removing unnecessary barriers to investment we further both objectives.

So why focus on competitiveness and productive investment today? Apart from being front of mind in most of my discussions with the insurance sector, they feature amongst the principles the PRA 'has regard to' when making rules or designing policy.

Matters that PRA 'has regard to' serve to focus the decision-makers' minds in weighing up how best to advance the PRA's objectives given to us in law.

To put this more colloquially, the PRA does not make rules or design policy solely in pursuit of a secondary objective or the goals underlying a 'have regard'.

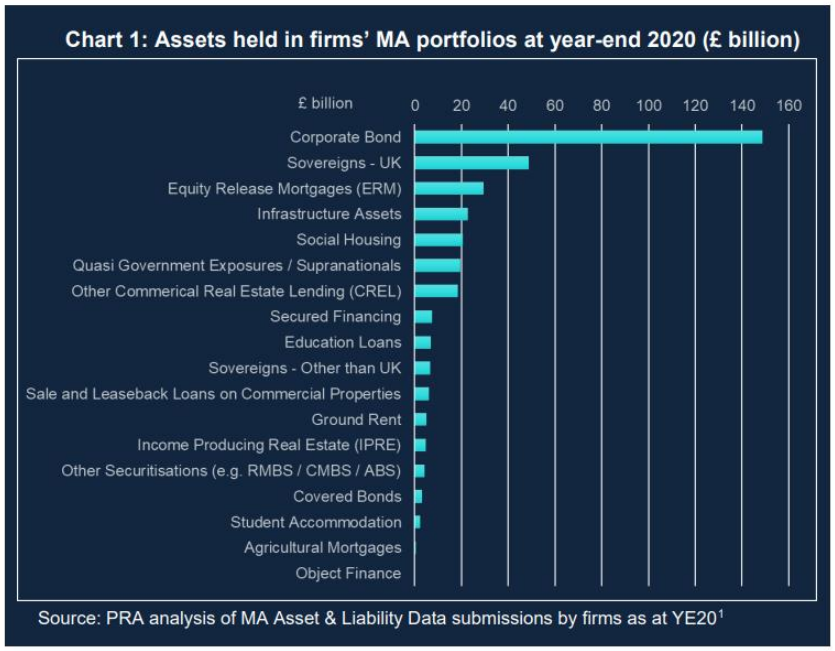
Rather, the existing secondary competition objective, and also the principles underlying our 'have regards' shape how we go about advancing our primary objectives.

We have thought carefully about the impact of our potential reforms in these areas. So, I want to explain how we're having regard to competitiveness and productive investment as we develop reform proposals.

Investment flexibility and productive investment

Looking first at investment flexibility. UK insurers manage almost £890bn of investment assets, and it is an objective of regulatory reform to support the productive investment of those funds.

In the UK, we have a strong flow of defined benefit pension liabilities to insurers, which provides a further incentive to ensure the regulatory regime can facilitate productive investments within the bounds of appropriate risk management of those funds.
To read more:
https://www.bankofengland.co.uk/speech/2022/june/charlotte-gerken-keynote-speaker-at-the-jp-morgan-european-insurance-conference



Number 3

Annual report 2021

EIOPA's Board of Supervisors (BoS) takes note of the Consolidated Annual Activity Report (CAAR) 2021, submitted by the Authorising Officer in accordance with Article 48(1) of the Financial Regulation (FR) applicable to EIOPA. Analysing and assessing the CAAR 2021 BoS has made the following observations:

1. The report contains a comprehensive and thorough account of the activities carried out by EIOPA in the implementation of its mandate and programme of work during 2021.

EIOPA has met its obligations under Article 48(1), providing a detailed account of the results achieved in relation to the objectives set in the Annual Work Programme 2021, financial and management information, as well as the risks related to the organisational activities and measures taken to address them.

2. BoS acknowledges that EIOPA delivered a very demanding Annual Work Programme that included work deprioritised in 2020 due to COVID-19 impact on its work.

3. BoS acknowledges the continued challenges EIOPA faces to manage a demanding workload towards monitoring and mitigating risks, supporting the recovery of the economy, assisting in building more resilient insurance and pensions sectors and further strengthening a common supervisory culture. The BoS welcomes EIOPA's efforts to prioritise in order to deal with a demanding workload and a challenging macro-economic environment.

4. BoS welcomes the significant contribution EIOPA has made in the field of conduct of business supervision and its work to address conduct risks for consumers through the use of EIOPA's product intervention powers and a range of supervisory and oversight tools, including the continued consumer trends and market monitoring work, and visits to national competent authorities (NCAs).

Furthermore, BoS welcomes EIOPA's work together with the other ESAs in developing regulatory technical standards for a targeted Level 2 Review on PRIIPs and for the Sustainable Finance Disclosure Regulation and Taxonomy Regulation.

Finally, the BoS welcomes the work initiated in 2021 on providing input to the Commission's call for advice on Retail Investor Protection and the review of the PRIIPs Regulation where a short deadline of 9 months is envisaged to complete the work by end of April 2022.

5. BoS welcomes EIOPA's continued contribution to building an effective and consistent level of supervision across the EU.

In particular, the ongoing focus on cross-border business, particularly with regards to EIOPA's cross-border cooperation platforms and work on cross-border cases with possible detriment to consumers. At the same time, the BoS acknowledges the limitation of EIOPA's toolbox and impact of the current European supervisory architecture.

6. BoS supports EIOPA's supervisory convergence plans and acknowledges the comprehensive set of objectives and activities established in these plans to achieve supervisory convergence.

In particular, BoS welcomes EIOPA's criteria for the independence of supervisory authorities, which is crucial for the legitimacy and credibility of the supervisory process.

7. BoS welcomes EIOPA's work on the monitoring of Solvency II. In particular, the report on the use of limitations and exemptions from reporting 2019-2020, on the use of capital add-ons during 2019 and 2020, on long-term guarantees measures and measures on equity risk 2020, and the report on European Insurance Overview (solo undertakings).

8. BoS welcomes EIOPA's technical advice on the development of Pension Tracking Systems providing a set of principles, good practices and recommendations, aiming to facilitate citizens' digital access to personal pension information.

BoS also welcomes EIOPA's technical advice on pensions dashboard with an aim to strengthen the monitoring of pension developments in the EU by presenting a complete set of indicators that allow for enhanced analysis and comparison and are also easy to comprehend.

9. BoS welcomes EIOPA's continued monitoring and analysis of vulnerabilities in the market and financial stability risks and in particular, EIOPA's quarterly risk dashboard and semi-annual financial stability reports.
BoS welcomes the 2021 stress test exercise that focused on a prolonged Covid-19 scenario targeting European (re)insurance groups and covering 75% of the EU-wide market based on total assets under Solvency II.

Furthermore, BoS welcomes additional areas of financial stability work such as the liquidity monitoring framework, the methodological framework for stress-testing IORPs setting out theoretical and practical rules, guidance and possible approaches to support future IORP stress test exercises.

10. BoS welcomes EIOPA's activities following the entry into force of the PEPP, including an efficient IT infrastructure and the development of a supervisory framework.

11. BoS welcomes EIOPA's achievements in the area of sustainable finance to support the European Commission's Sustainable Finance Agenda, including the Renewed Sustainable Finance Strategy, in striving for greater protection against climate and environmental risks through insurance coverage, and integrating sustainability risks to the prudential framework for insurers.

In particular, the BoS welcomes EIOPA's Opinion on the supervision of the use of climate change scenarios in Own Risk and Solvency Assessment (ORSA)10.

12. BoS also welcomes EIOPA's work on the use of digital technology identifying ways to better protect consumers without hindering innovation including work on Digital Ethics, open insurance, and the adoption and implementation of Guidelines on information and communication technology (ICT) security and governance.

BoS welcomes EIOPA's work, alongside ESMA and EBA, in preparing a response to the European Commission's Call for the Advice on the Digital Finance Strategy, providing technical input on issues with changing value chains in the insurance sector, the emergence of platforms and the supervision of entities undertaking mixed activities.

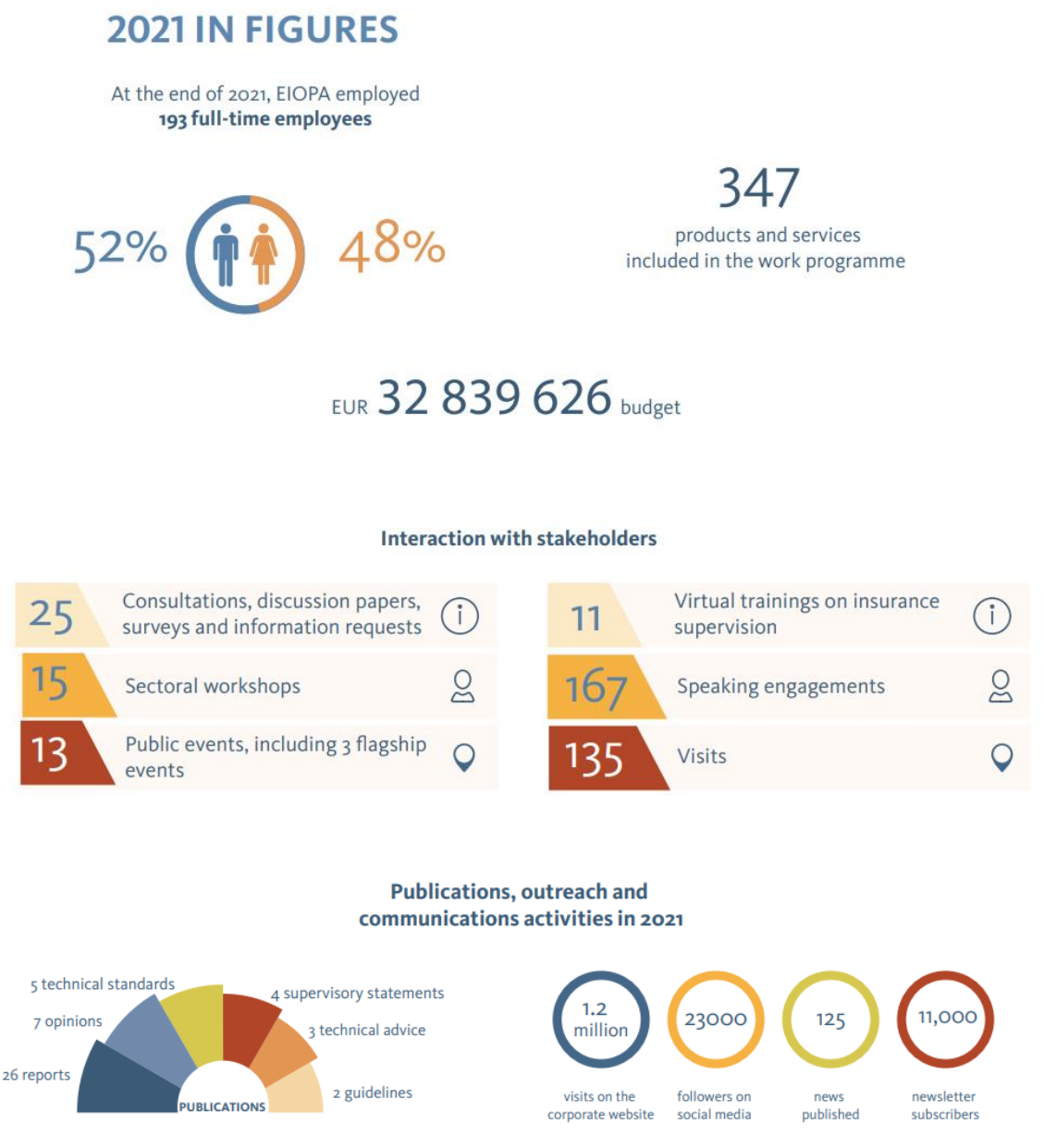
13. BoS notes the positive results of successful management of the Authority's tasks and resources, indicated by the high rate of delivery of products and services as planned or within a minor delay, as well as the targets met in terms of EIOPA's key performance indicators on management of its financial resources.

14. BoS notes EIOPA's diligent response to findings from the European Court of Auditors, the Internal Audit Service and the Authority's Quality Control Committee and supports EIOPA's efforts in its transparent implementation of the respective recommendations.

15. BoS considers that EIOPA is running effectively and efficiently and is delivering the expected products and services to high standards of quality.

Petra Hielkema
Chairperson of the Board of Supervisors

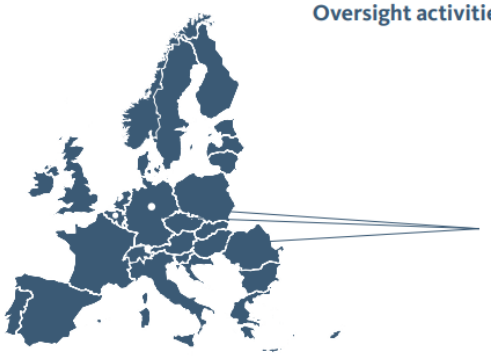
To read more:
https://www.eiopa.europa.eu/sites/default/files/publications/annual_reports/2021-eiopa-annual-report.pdf



The 2021 insurance stress test involved

44	117	20	75%
(re)insurers for the capital component	solo undertakings for the liquidity component	jurisdictions	market coverage in EEA based on total assets

Oversight activities at a glance



3 Joint on-site inspections on companies based in Germany, Liechtenstein and Luxembourg

80	56	11	23
colleges of supervisors meetings	involving insurance groups	cooperation platforms	participating National Supervisory Authorities

243	Q&As	143
questions on regulation were closed in 2021	on regulation	questions were sent to EIOPA

Number 4

Annual report 2021

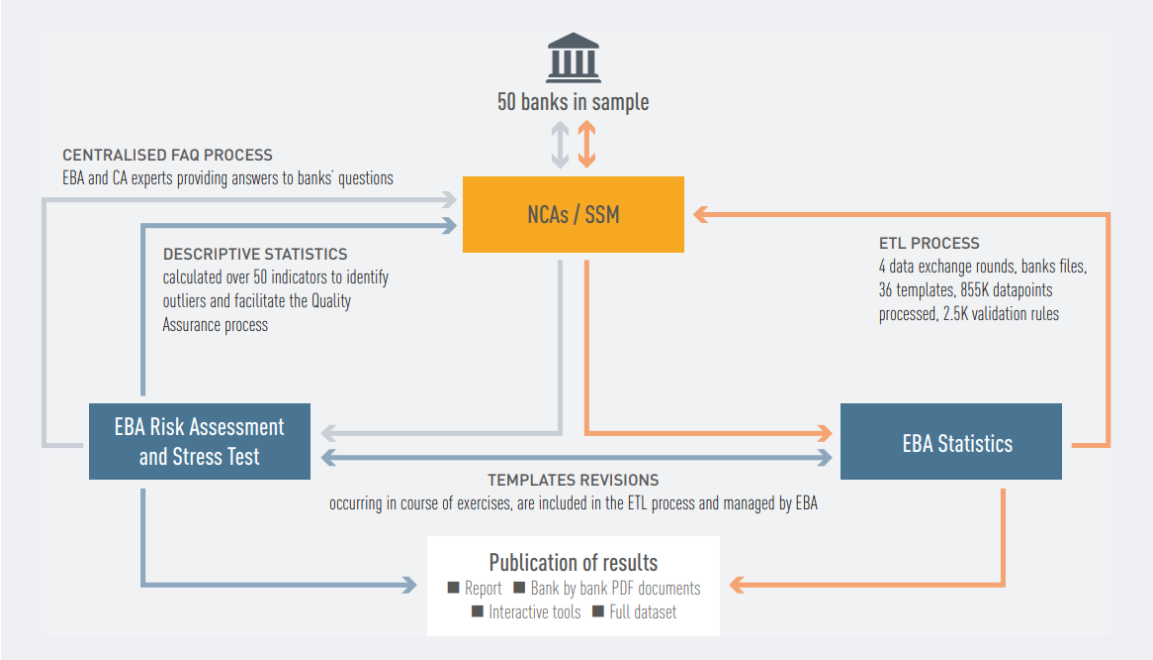
Identifying, assessing and monitoring risks in the EU banking sector

Improving the EU-wide stress testing framework

In line with the feedback received on the discussion paper on the future changes to the EU-wide stress testing framework, the EBA Board of Supervisors supported the exploration and implementation of a hybrid approach.

While the status quo remains an option in the short term, the hybrid approach will mean that some selected elements will follow a centralised approach while the rest of the methodology will remain inherently bottom-up.

Investigating the role of top-down elements in the EU-wide stress test



The EBA Board of Supervisors has identified net interest income and net fee and commission income as suitable candidates for centralisation, potentially for the 2023 EU-wide stress test exercise.

Due to the strict timelines for the finalisation of the methodology for the 2023 EU-wide stress test, the EBA Board of Supervisors decided to continue working in parallel on the bottom-up methodology considering the lessons learned in the 2021 EUwide stress test exercise.

A final decision on the implementation of some top-down elements in the 2023 EU-wide stress test is expected in the second quarter of 2022.

THE 2021 EU-WIDE STRESS TEST: ASSESSING BANKS' CAPACITY TO WITHSTAND FURTHER SHOCKS

In July 2021, the EBA published the results of the 2021 EU-wide stress test, which involved 50 banks covering broadly 70% of total EU banking sector assets.

The 2021 EU-wide stress test exercise was initially planned for 2020 but postponed to allow banks to prioritise operational continuity while the COVID-19 pandemic was unfolding.

The stress test helped supervisors assess banks' capacity to withstand further shocks. Given the unprecedented macroeconomic shock due to the pandemic in 2020, the baseline scenario provided a useful yardstick for assessing and comparing the situation of EU banks, assuming an orderly exit from the pandemic.

Hence, the stress test also helped provide a perspective on how the banking system could develop after the pandemic.

During 2020, EU banks continued to build up their capital base, with a CET1 ratio at the beginning of the exercise (i.e. at the end of 2020) of 15%, the highest since the EBA has been performing stress tests, despite the unprecedented decline in gross domestic product (GDP) and the initial effects of the COVID-19 pandemic in that year.

Under the adverse scenario, the average impact on the EU banking system was equal to a 485 bp decline in the CET1 fully loaded ratio for banks.

In the baseline scenario, banks' CET1 fully loaded ratio increased by 78 bps, bringing the sector's average CET1 fully loaded ratio to 15.8% at the end of 2023.

It is encouraging to see that overall, EU banks in aggregate remained above the 10% mark and hence would be able to continue lending despite a very severe adverse scenario.

In line with previous exercises, the EBA published granular stress test data at a bank-by-bank level, which is a must for fostering market discipline at times of increased uncertainty in the markets, while the results of the exercise represent a key input to the supervisory review and evaluation process (SREP).

The EBA is responsible for initiating and coordinating the EU-wide stress test, supplying the methodology, working with the ESRB and the ECB to provide a common scenario and publishing the results, including a report and granular bank-by-bank data together with analytical interactive tools.

During the exercise, the EBA, together with the supervisory authorities, closely manage the data extraction, transformation, and loading (ETL) process to ensure a high level of data quality.

More than 850,000 data points are processed and around 2,500 validation rules ensure that this is carried out properly. While the supervisory authorities take responsibility for ensuring the quality of the submissions received from banks with the results, the EBA facilitates the process by providing descriptive statistics and managing the process of clarifying methodological questions from banks through a centralised FAQ process.

To read more:
https://www.eba.europa.eu/sites/default/documents/files/document_library/About%20Us/Annual%20Reports/2021/1035237/EBA%202021%20Annual%20Report.pdf

Number 5

Welcoming remarks

International Roles of the US Dollar conference

Jerome H Powell, Chair of the Board of Governors of the Federal Reserve System, at "International Roles of the US Dollar", a research conference sponsored by the Federal Reserve Board, Washington DC.

Good morning, and welcome to the inaugural conference on the International Roles of the U.S. Dollar. Thank you all for participating and for lending your expertise on this important topic. This conference marks the first use of our new Martin Conference Center, which I hope you enjoy.

The international financial and monetary system that emerged after World War II has been defined by the centrality of the dollar.

It is the world's reserve currency and the most widely used for payments and investments.

As outlined in recent work by Board staff, this global preeminence has been supported by the depth and liquidity of U.S. financial markets, the size and strength of the U.S. economy, its stability and openness to trade and capital flows, and international trust in U.S. institutions and the rule of law.

Professor Barry Eichengreen will expand on some of these themes later this morning.

The dollar's international role holds multiple benefits. For the United States, it lowers transaction fees and borrowing costs for U.S. households, businesses, and the government.

Its ubiquity helps contain uncertainty and, relatedly, the cost of hedging for domestic households and businesses. For foreign economies, the wide use of the dollar allows borrowers to have access to a broad pool of lenders and investors, which reduces their funding and transaction costs.

The benefits of the dollar as the dominant reserve currency have generated an extensive academic literature. Yesterday's paper on the Treasury market by Alexandra Tabova and Frank Warnock extends that work in meaningful ways.

The Federal Reserve's strong commitment to our price stability mandate contributes to the widespread confidence in the dollar as a store of value. To that end, my colleagues and I are acutely focused on returning inflation to our 2 percent objective.

Meeting our dual mandate also depends on maintaining financial stability. The Fed's commitment to both our dual mandate and financial stability encourages the international community to hold and use dollars.

The wide use of the dollar globally can also pose financial stability challenges that can materially affect households, businesses, and markets.

For that reason, the Federal Reserve has played a key role in promoting financial stability and supporting the use of dollars internationally through our liquidity facilities.

The central bank liquidity swap lines provide foreign central banks with the capacity to deliver U.S. dollar funding to institutions in their jurisdictions.

And the Foreign and International Monetary Authorities (FIMA) Repo Facility allows approved FIMA account holders the option to temporarily exchange their U.S. Treasury securities held by the Federal Reserve for U.S. dollars.

These facilities serve as liquidity backstops so that holders of dollar assets and participants in dollar funding markets can be confident that strains will be eased when these markets come under stress.

That assurance, in turn, mitigates the effect of such strains on the flow of credit to U.S. households and businesses. Both facilities enhance the standing of the dollar as the dominant global currency.

The swap lines were extensively used during the Global Financial Crisis, the 2011 euro-area debt crisis, and the financial turmoil at the outset of the COVID-19 pandemic in 2020.

The paper on central bank swap lines presented yesterday by Gerardo Ferrara, Philippe Mueller, Ganesh Viswanath-Natraj, and Junxuan Wang provides novel micro-level evidence on the usefulness of swap lines in providing cross-border liquidity to support the real economy.

Looking forward, rapid changes are taking place in the global monetary system that may affect the international role of the dollar in the future. Most major economies already have or are in the process of developing instant, 24/7 payments.

Our own FedNow service will be coming online in 2023. And in light of the tremendous growth in crypto-assets and stablecoins, the Federal Reserve is examining whether a U.S. central bank digital currency (CBDC) would improve on an already safe and efficient domestic payments system. As the Fed's white paper on this topic notes, a U.S. CBDC could also potentially help maintain the dollar's international standing.

As we consider feedback from the paper, we will be thinking not just about the current state of the world, but also how the global financial system might evolve over the next 5 to 10 years. The paper by Jiakai Chen and Asani Sarkar, which is on today's program, and our distinguished panelists on this topic this afternoon, will provide important insights on this issue.

To summarize, I would like to stress the importance of the dollar to the U.S. and global economies and financial markets. It is critical that we understand the channels, connections, and effects of the role of the dollar.

In closing, I want to thank you all for taking the time to join our discussion on the dollar's international roles. This conference brings together world-class researchers, practitioners, and policymakers dedicated to understanding and addressing these vital issues. I look forward to their insights and I hope you enjoy the conference.

To read more: https://www.bis.org/review/r220620i.htm

Number 6

Botnet Disrupted in International Cyber Operation

THE UNITED STATES ATTORNEY'S OFFICE
SOUTHERN DISTRICT of CALIFORNIA

The U.S. Department of Justice, together with law enforcement partners in Germany, the Netherlands and the United Kingdom, have dismantled the infrastructure of a Russian botnet known as RSOCKS which hacked millions of computers and other electronic devices around the world.

A botnet is a group of hacked internet-connected devices that are controlled as a group without the owner's knowledge and typically used for malicious purposes. Every device that is connected to the internet is assigned an Internet Protocol (IP) address.

According to a search warrant affidavit, unsealed today in the Southern District of California, and the operators' own claims, the RSOCKS botnet, operated by Russian cybercriminals, comprised millions of hacked devices worldwide.

The RSOCKS botnet initially targeted Internet of Things (IoT) devices. IoT devices include a broad range of devices—including industrial control systems, time clocks, routers, audio/video streaming devices, and smart garage door openers, which are connected to, and can communicate over, the internet, and therefore, are assigned IP addresses.

The RSOCKS botnet expanded into compromising additional types of devices, including Android devices and conventional computers.

"The RSOCKS botnet compromised millions of devices throughout the world," said U.S. Attorney Randy Grossman. "Cyber criminals will not escape justice regardless of where they operate. Working with public and private partners around the globe, we will relentlessly pursue them while using all the tools at our disposal to disrupt their threats and prosecute those responsible." Grossman thanked the prosecution team, the FBI and the Department of Justice Criminal Division's Computer Crimes and Intellectual Property Section for their excellent work on this case.

"This operation disrupted a highly sophisticated Russia-based cybercrime organization that conducted cyber intrusions in the United States and abroad," said FBI Special Agent in Charge Stacey Moy. "Our fight against cybercriminal platforms is a critical component in ensuring cybersecurity and safety in the United States. The actions we are announcing today are a testament to the FBI's ongoing commitment to pursuing foreign threat actors in collaboration with our international and private sector partners."

A legitimate proxy service provides IP addresses to its clients for a fee. Typically, the proxy service provides access to IP addresses that it leases from internet service providers (ISPs). Rather than offer proxies that RSOCKS had leased, the RSOCKS botnet offered its clients access to IP addresses assigned to devices that had been hacked.

The owners of these devices did not give the RSOCKS operator(s) authority to access their devices in order to use their IP addresses and route internet traffic.

A cybercriminal who wanted to utilize the RSOCKS platform could use a web browser to navigate to a web-based "storefront" (i.e., a public web site that allows users to purchase access to the botnet), which allowed the customer to pay to rent access to a pool of proxies for a specified daily, weekly, or monthly time period.

The cost for access to a pool of RSOCKS proxies ranged from $30 per day for access to 2,000 proxies to $200 per day for access to 90,000 proxies.

Once purchased, the customer could download a list of IP addresses and ports associated with one or more of the botnet's backend servers. The customer could then route malicious internet traffic through the compromised victim devices to mask or hide the true source of the traffic.

It is believed that the users of this type of proxy service were conducting large scale attacks against authentication services, also known as credential stuffing, and anonymizing themselves when accessing compromised social media accounts, or sending malicious email, such as phishing messages.

As alleged in the unsealed warrant, FBI investigators used undercover purchases to obtain access to the RSOCKS botnet in order to identify its backend infrastructure and its victims.

The initial undercover purchase in early 2017 identified approximately 325,000 compromised victim devices throughout the world with numerous devices located within San Diego County.

Through analysis of the victim devices, investigators determined that the RSOCKS botnet compromised the victim device by conducting brute force attacks.

The RSOCKS backend servers maintained a persistent connection to the compromised device. Several large public and private entities have been victims of the RSOCKS botnet, including a university, a hotel, a television studio, and an electronics manufacturer, as well as home businesses and

individuals. At three of the victim locations, with consent, investigators replaced the compromised devices with government-controlled computers (i.e., honeypots), and all three were subsequently compromised by RSOCKS. The FBI identified at least six victims in San Diego.

This case was investigated by the FBI and is being prosecuted by Assistant U.S. Attorney Jonathan I. Shapiro of the Southern District of California and Ryan K.J. Dickey, Senior Counsel for the Department of Justice Criminal Division's Computer Crimes and Intellectual Property Section. The Department of Justice extends its appreciation to the authorities of Germany, the Netherlands, and the United Kingdom, the Justice Department's Office of International Affairs and private sector cybersecurity company Black Echo, LLC for their assistance provided throughout the investigation.

In September 2020, FBI Director Christopher Wray announced the FBI's new strategy for countering cyber threats. The strategy focuses on imposing risk and consequences on cyber adversaries through the FBI's unique authorities, world-class capabilities, and enduring partnerships. Victims are encouraged to report the incident online with the Internet Crime Complaint Center (IC3) www.ic3.gov

To read more:
https://www.justice.gov/usao-sdca/pr/russian-botnet-disrupted-international-cyber-operation

Number 7

FBI Las Vegas Federal Fact Friday:
Social Media Money Flipping Scam

The FBI Las Vegas Field Office wants to educate the public about a scam taking place using social media platforms and banking apps to solicit large sums of cash from victims.

Money Flipping

The FBI has alerted social media companies of a series of legitimate accounts being hijacked by scammers advertising unrealistic money flipping opportunities.

These scammers claim they will exponentially increase a victim's funds once provided via Cash App. These scammers will often have legitimate-looking profiles displaying strangers with large sums of cash resulting from their participation in the fraudulent investment.

How It is Implemented

Scammers contact the victim directly via private messenger, often using accounts stolen from the victim's friends.

The scammers will offer returns larger than the victim's investment at no interest and no risk.

If the victim sends money, communications are either ceased or scammers will send fake Cash App screenshots indicating the victim's money has already increased.

They then request more money with the promise of more returns that the victim will never see.

If the victim sent money or not, the scammers often suggest money is pending in the victim's Cash App account but requires replacing the email address connected to the victim's social media account with one provided by the scammers.

Once done, the scammers reset the password and take control of the account. Once they have control, the cycle continues, now against the victim's followers.

Means Of Defense

Use dual-factor authentication (DFA) when available. Though many find this inconvenient, having DFA prevents accounts from being hijacked simply by email reset. This helps prevent many forms of account hijacking and can also alert users of hijack attempts.

Do not change your account information based on outside requests. There is no legitimate reason to change your account information to that of someone else's. Cash App is not locked by social media settings and anyone that attempts to convince you otherwise is likely attempting to gain access to your information. Be cautious.

Do not click on links and verify who you're conversing with. If you are having an unusual conversation with someone on social media and they attempt to solicit money or account information, question this and give them a phone call.

Talk to your friends live, ask questions, be skeptical, and do not click on links as they may be directing you to a malicious webpage.

Online, anyone can be anyone else. Trust, but verify. If the money transfer application has a security pin feature that requires PIN entry before authorizing a transfer, use it!

Number 8

Miners as intermediaries: extractable value and market manipulation in crypto and DeFi

BIS Bulletin 58, Raphael Auer, Jon Frost and Jose María Vidal Pastor

BIS

Key takeaways

• Cryptocurrencies such as Ethereum and decentralised finance (DeFi) protocols built on them rely on validators or "miners" as intermediaries to verify transactions and update the ledger.

• Since these intermediaries can choose which transactions they add to the ledger and in which order, they can engage in activities that would be illegal in traditional markets such as front-running and sandwich trades. The resulting profit is termed "miner extractable value" (MEV).

• MEV is an intrinsic shortcoming of pseudo-anonymous blockchains. Addressing this form of market manipulation may call for new regulatory approaches to this new class of intermediaries.

Far from being "trustless", cryptocurrencies and decentralised finance (DeFi) rely on intermediaries who must be incentivised to maintain the ledger of transactions.

Yet each of the validators or "miners" updating the blockchain can determine which transactions are executed and when, thus affecting market prices and opening the door to front-running and other forms of market manipulation.

These intrinsic shortcomings of permissionless blockchain technology are well known in the field of computer science and the cryptocurrency industry (see Daian et al (2020)).

In fact, a new term has been coined for the profits that miners can make via their ability to choose which transactions to include and in which order: *"miner extractable value" (MEV).*

This is defined as the profit that miners can take from other investors by manipulating the choice and sequencing of transactions added to the blockchain. This bulletin explains MEV and why it arises, documents the amounts involved, and draws regulatory implications for cryptocurrencies, DeFi and other blockchain-based applications.

What is MEV and why does it arise?

In traditional financial markets, user transactions are sequenced by a trusted and regulated intermediary in the order in which they are received.

In a blockchain, by contrast, the updating of a block is competitive and random. For example, in a cryptocurrency based on proof-of-work such as Bitcoin, all miners use their computing power to quickly solve a puzzle that will allow only one of them to add the next block (see Auer (2019)).

The probability that a given miner will add the next block is equal to that miner's share in the total computing power expended.

This process can be considered "decentralised" and equitable in the sense that there are many different miners, and no single miner can censor a specific transaction forever.

This is because, if the fee that a transaction pays is high enough, some other miner will eventually include it in the block.

Similar arguments hold for a proof-of-stake-based network, into which the Ethereum network aims to transition.

Still, when a miner can add a new block, they are free to assemble this block in any way they want. This lets them extract value from other users.

Beside collected legitimate transaction fees (eg the "gas" fees in Ethereum), they can assemble their block from all pending transactions – the memory pool or "mempool" – in such a way as to maximise MEV. The latter are profits that are made by manipulating market prices via a specific ordering – or even censoring – of pending transactions.

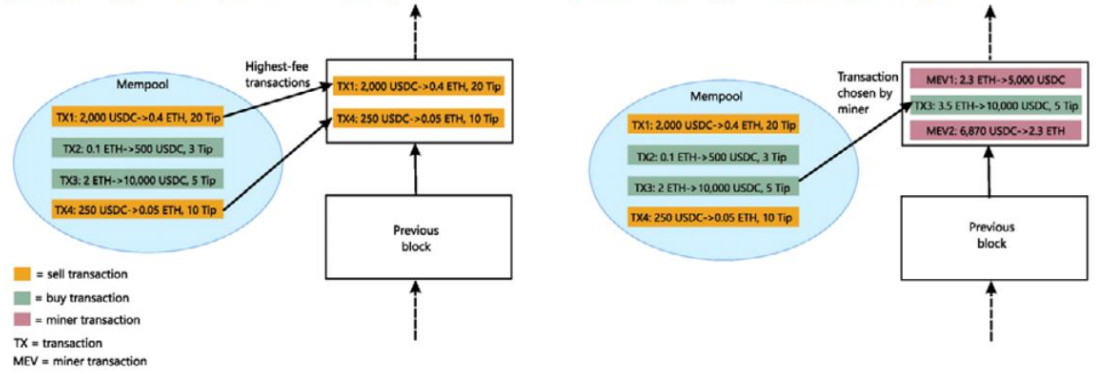
Because the ledger is publicly observable, these forms of market manipulation can be seen, even if the underlying identity of the miners or other parties in question is unknown.

Graph 1 illustrates a hypothetical example of a sandwich trade by a miner with transactions in the stablecoin USD Coin (USDC) and Ethereum's cryptocurrency Ether (ETH).

Several different users put in buy and sell transactions in the mempool, and the miner can select which orders to include in this block. In theory, miners should select and order transactions based on fees only (left-hand panel). As each Ethereum transaction needs computing power and resources to be executed, a fee is paid to the miners to execute the transaction, paid in small

units of ETH (gigawei or "gwei", each equal to 0.000000001 ETH). Total fees are the sum of a base fee (which is destroyed or "burned") plus a priority fee ("Tip", decided by the user when sending the transaction to the mempool).

Fee-based mining allows for value extraction — Graph 1



[1] The mempool contains various signed but pending transactions, which are ordered and added to the next block according to the amount of Tip, whether or not it is a buy or a sell order, assuming a constant base gas fee.[2] Miners add their own transactions to the block to profit from a different ordering of pending transactions based on the size and direction of the largest-volume transaction, therefore altering its market price and benefiting from a trading advantage.

Source: Authors' elaboration.

To read more: https://www.bis.org/publ/bisbull58.pdf

Number 9

NIST Releases Draft IR 8409

Measuring the Common Vulnerability Scoring System Base Score Equation

NIST is seeking public comments on NIST IR 8409 ipd (initial public draft), Measuring the Common Vulnerability Scoring System Base Score Equation.

Calculating the severity of information technology vulnerabilities is important for prioritizing vulnerability remediation and helping to understand the risk of a vulnerability.

The Common Vulnerability Scoring System (CVSS) is a widely used approach to evaluating properties that lead to a successful attack and the effects of a successful exploitation.

CVSS is managed under the auspices of the Forum of Incident Response and Security Teams (FIRST) and is maintained by the CVSS Special Interest Group (SIG).

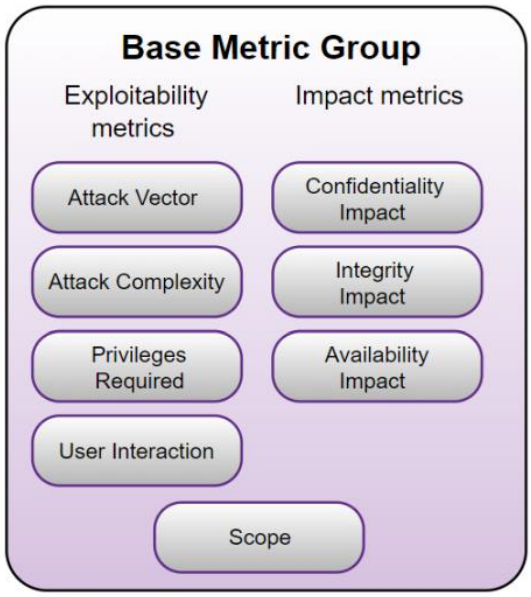
Unfortunately, ground truth upon which to base the CVSS measurements has not been available. Thus, CVSS SIG incident response experts maintain the equations by leveraging CVSS SIG human expert opinion.

This work evaluates the accuracy of the CVSS “base score” equations and shows that they represent the CVSS maintainers' expert opinion to the extent described by these measurements.

NIST requests feedback on the approach, the significance of the results, and any CVSS measurements that should have been conducted but were not included within the initial scope of this work.

Finally, NIST requests comments on sources of data that could provide ground truth for these types of measurements.

The public comment review period for this draft is open through *July 29,* 2022. See the publication details for instructions on how to submit comments.



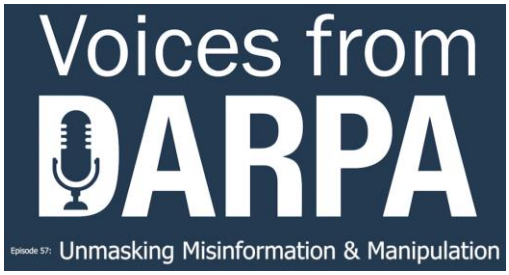
To read more:
https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8409.ipd.pdf

Number 10

Voices from DARPA Podcast Episode 57

Unmasking Misinformation & Manipulation

In this 20-minute episode of the Voices from DARPA podcast, we discuss DARPA's Influence Campaign Awareness and Sensemaking (INCAS) program.



Adversaries exploit misinformation and true information through compelling narratives propagated on social media and online content.

INCAS seeks new tools to help analysts quickly identify geopolitical influence campaigns amidst today's noisy information environment and find better ways to determine the impacts of such propaganda.

We talk with leaders of teams working on aspects of the INCAS program – including identifying narratives using lessons from the entertainment industry and exploring how different people react to the same messages – in addition to INCAS Program Manager Brian Kettler.

As Kettler says: "Propaganda is not new, but the speed and scale of it is new. The information ecosystem is rapidly evolving. Our adversaries are getting better all the time."

You may visit: https://youtu.be/g9aoZiP48Fc

https://itunes.apple.com/us/podcast/voices-from-darpa/id1163190520

Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any individual or entity;

- should not be relied on in the context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of an interpretative document;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors.

However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

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

International Association of Risk and Compliance Professionals (IARCP)

You can explore what we offer to our members:

1. *Membership* – Become a standard, premium or lifetime member.

You may visit:
https://www.risk-compliance-association.com/How_to_become_member.htm

2. *Weekly Updates* - Visit the *Reading Room* of the association at:
https://www.risk-compliance-association.com/Reading_Room.htm

3. *Training and Certification* – Become:

- a Certified Risk and Compliance Management Professional (CRCMP),

- a Certified Information Systems Risk and Compliance Professional (CISRCP),

- a Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P,

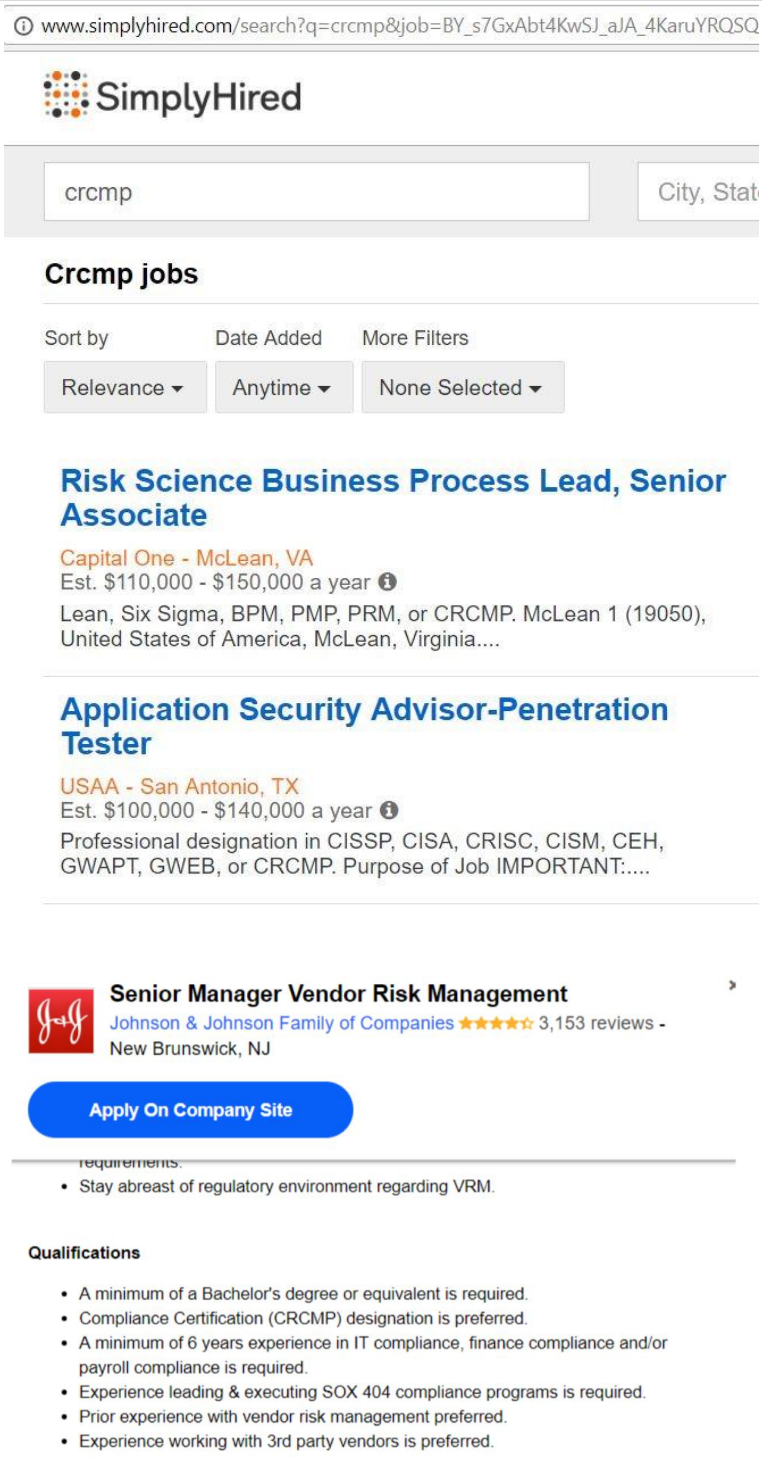
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- a Travel Security Trained Professional (TSecTPro).

The CRCMP has become one of the most recognized certificates in risk management and compliance. There are CRCMPs in 32 countries.

Companies and organizations around the world consider the CRCMP a preferred certificate:

Senior Information Security Risk Analyst
Public Company Accounting Oversight Board - ★★★★☆ 10 reviews - Washington, DC
Professional designation in CISSP, CISA, CRISC, or CRCMP preferred. The PCAOB is a nonprofit corporation established by Congress to oversee the audits of public...



You can find more about the demand for CRCMPs at:
https://www.risk-compliance-association.com/CRCMP_Jobs_Careers.pdf

For the Certified Risk and Compliance Management Professional (CRCMP) distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/Distance_Learning_and_Certification.htm

For the Certified Information Systems Risk and Compliance Professional (CISRCP), distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CISRCP_Distance_Learning_and_Certification.htm

For the Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P, distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CC_GRC_P_Distance_Learning_and_Certification.htm

For the Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CRCMP_Re_I.htm

For the Travel Security Trained Professional (TSecTPro), distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/TSecTPro_Distance_Learning_and_Certification.htm

Certified Cyber (Governance Risk and Compliance) Professionals - CC(GRC)Ps, have a 50% discount for the Travel Security Trained Professional (TSecTPro) program ($148 instead of $297).

You have a $100 discount after you purchase one of our programs. The discount applies to each additional program. For example, you can purchase the CRCMP program for $297, and then purchase the CISRCP program for $197 (instead of $297), the CC(GRC)P program for $197 (instead of $297), the CRCMP(Re)I program for $197 (instead of $297), and the TSecTPro program for $197 (instead of $297).

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