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, April 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,

I have just read the new "Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP) and supervisory stress testing" from the European Banking Authority (EBA). I read (again) some interesting definitions from the EBA.

According to the paper, *'Conduct risk'* means the current or prospective risk of losses to an institution arising from cases of wilful or negligent misconduct, including inappropriate supply of financial services.

According to the Chartered Institute of Internal Auditors (2018), *'Conduct risk'* is the risk associated to the way organizations, and their staff, relate to customers and the wider financial markets.

The UK Financial Conduct Authority (FCA), in its *Retail Conduct Risk Outlook 2011,* referred to conduct risk as the risk that firm behaviour will

result in poor outcomes for customers. Good customer outcomes may be defined as customers getting financial services and products that meet their needs.

According to KPMG, in the paper *Conduct risk: delivering an effective framework,* conduct risk is broadly defined as any action of a financial institution or individual that leads to customer detriment, or has an adverse effect on market stability or effective competition. They are right when they add that "the FCA has deliberately set out a very wide definition of 'conduct risk', leaving the onus on financial services firms to prove how they are protecting customers".

There are many other definitions. According to Lao Tzu, "When virtue is lost, benevolence appears, when benevolence is lost right conduct appears, when right conduct is lost, expedience appears. Expediency is the mere shadow of right and truth; it is the beginning of disorder".

Read more at number 2 below. Welcome to our 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 23)

From open banking to open finance

Denis Beau, First Deputy Governor of the Bank of France, at the France Payments Forum "The Europe of banking and financial services" – Paris

Number 7 (Page 30)

Record-breaking, ultrafast devices step to protecting the grid from EMPs

New Sandia diode can shunt excess electricity in a few billionths of a second

Sandia National Laboratories

Number 8 (Page 35)

Consumers warned about chatbot scam

National Cyber Security Centre

Number 9 (Page 37)

There's More to AI Bias Than Biased Data

Rooting out bias in artificial intelligence will require addressing human and systemic biases as well.

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

Number 10 (Page 40)

Voices from DARPA Podcast Episode 54: Climate Tipping Points

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 1

Warning to consumers on the risks of crypto-assets

The European Supervisory Authorities (EBA, ESMA and EIOPA – the ESAs) warn consumers that many crypto-assets are highly risky and speculative. The ESAs set out key steps consumers can take to ensure they make informed decisions.

This warning comes in the context of growing consumer activity and interest in crypto-assets and the aggressive promotion of those assets and related products to the public, including through social media.

You should be aware of the specific risks of crypto-assets and related products and services and carefully weigh up whether the risks are acceptable given your own preferences and financial situation.

These include the risk that:

• you may lose all the money you invest;

• prices can fall and rise quickly over short periods;

• you may fall victim to scams, fraud, operational errors or cyber attacks;

• you are unlikely to have any rights to protection or compensation if things go wrong.

If you are thinking about buying crypto-assets or related products and services, you should ask yourself the following:

• can you afford to lose all the money you invest?

• are you ready to take on high risks to earn the advertised returns?

• do you understand the features of the crypto-asset or related products and services?

• are the firms/parties you are dealing with reputable?

• are the firms/parties you are dealing with blacklisted by the relevant national authorities?

• are you able to protect effectively the devices you use for buying, storing or transferring crypto-assets, including your private keys?

What are the key risks?

• *Extreme price movements:* many crypto-assets are subject to sudden and extreme price movements and are speculative, because their price often relies solely on consumer demand (i.e., there may be no backing assets or other tangible value).

You may lose a large amount or even all of the money invested. The extreme price movements also mean that many crypto-assets are unsuitable as a store of value, and as a means of exchange or payment;

• *Misleading information:* some crypto-assets and related products are aggressively advertised to the public, using marketing material and other information that may be unclear, incomplete, inaccurate or even purposefully misleading.

For instance, advertisements via social media may be very short, with a focus on the potential gains but not the high risks involved. You should also beware of social media 'influencers' who typically have a financial incentive to market certain crypto-assets and related products and services and therefore may be biased in the communications they issue;

• *Absence of protection:* the majority of crypto-assets and the selling of products or services in relation to crypto-assets are unregulated in the EU.

In these cases you will not benefit from the rights and protections available to consumers for regulated financial services, such as complaints or recourse mechanisms;

• *Product complexity:* some products providing exposure to crypto-assets are very complex, sometimes with features that can increase the magnitude of losses in case of adverse price movements. These products, given their complexity, are not suitable for many consumers;

• *Fraud and malicious activities:* numerous fake crypto-assets and scams exist and you should be aware that their sole purpose is to deprive you of your money using different techniques, for example phishing;

• *Market manipulation, lack of price transparency and low liquidity:* how cryptoassets prices are determined and the execution of transactions at exchanges is often not transparent.

The holding of certain crypto-assets is also highly concentrated, which may impact prices or liquidity. You may therefore not get a fair price or treatment when buying or selling crypto-assets, or not be able to sell your crypto-assets as quickly as you would want in the absence of a potential buyer. Cases of market manipulation have been reported on multiple occasions; and

• *Hacks, operational risks and security issues:* the distributed ledger technology underpinning crypto-assets can bear specific risks. Several issuers and service providers for crypto-assets, including crypto exchanges and wallet providers, have experienced cyber-attacks and severe operational problems.

Many consumers have lost their crypto-assets or suffered losses due to such hacks and disruptions or because they have lost the private keys providing access to their assets.

You may visit:
https://www.eiopa.europa.eu/document-library/consumer-warnings/warning-consumers-risks-of-crypto-assets_en

Number 2

EBA publishes revised Guidelines on common procedures and methodologies for the supervisory review and evaluation process

The European Banking Authority (EBA) published its final revised Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP) and supervisory stress testing.

The revisions aim at implementing the amendments to the Capital Requirements Directive (CRD V) and Capital Requirements Regulation (CRR II) and promoting convergence towards best supervisory practices.

The changes to these Guidelines do not alter the overall SREP framework but affect its main elements, including:

(i) business model analysis,

(ii) assessment of internal governance and institution-wide control arrangements,

(iii) assessment of risks to capital and adequacy of capital to cover these risks, and

(iv) assessment of risks to liquidity and funding and adequacy of liquidity resources to cover these risks.

The main amendments are aiming at:

- better articulating the principle of proportionality, through the categorisation of institutions and the application of the minimum engagement model;

- fully incorporating the assessment of the money laundering and terrorist financing (ML/TF) risks, in line with the EBA Opinion on how to take into account ML/TF risks in the SREP;

- reviewing the provisions on Pillar 2 capital add-ons and the Pillar 2 guidance, to ensure they reflect a purely micro-prudential perspective and appropriately implement the separate stack of own funds requirements based on the leverage ratio;

- aligning the assessment of the interest rate risk in the non-trading book, as well as the assessment of liquidity risk and liquidity adequacy with the current regulatory framework;

- enhancing the dialogue among institutions and supervisors in relation to the setting of the Pillar 2 requirements.

Legal basis and background

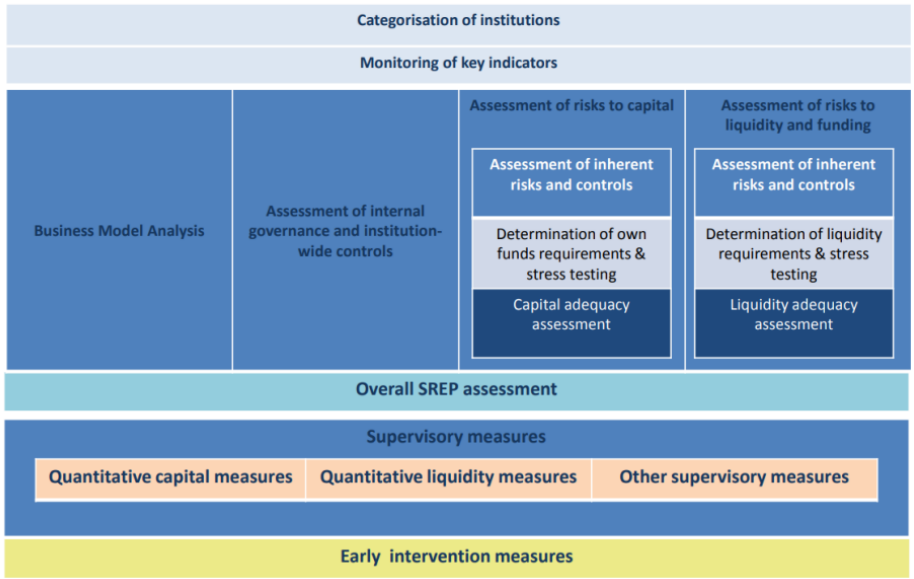
The EBA has developed these Guidelines in accordance with Article 107(3) of the CRD, which mandates the Authority to foster sound and effective supervision and to drive supervisory convergence across the EU. These Guidelines are addressed to all competent authorities across the EU.

SREP is an ongoing supervisory process bringing together findings from all supervisory activities into an institution's comprehensive supervisory overview.

These Guidelines also aim at achieving convergence of practices followed by competent authorities in supervisory stress testing across the EU in accordance with Article 100 of Directive 2013/36/EU.

To read more:
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2022/EBA-GL-2022-03%20Revised%20SREP%20Guidelines/1028500/Final%20Report%20on%20Guidelines%20on%20common%20procedures%20and%20methodologies%20for%20SREP%20and%20supervisory%20stress%20testing.pdf

Figure 1. Overview of the common SREP framework



Number 3

Full disclosure - coming to grips with an inconvenient truth

Frank Elderson, Member of the Executive Board of the European Central Bank and Vice-Chair of the Supervisory Board of the ECB, at the 14th European Bank Institute Policy Webinar on the ECB's supervisory approach on climate-related and environmental risks, Frankfurt am Main

Some years ago, Andrea Enria, the Chair of the Supervisory Board, gave a speech, precisely at an EBI conference, calling for greater transparency in prudential supervision.

When describing the role of transparency and information disclosure, he echoed the words of Supreme Court Justice Louis Brandeis:

"Sunlight is said to be the best of disinfectants; electric light the most efficient policeman".

This couldn't be truer for climate-related disclosures, too. As I have said before when discussing the supervision and prominence of climate-related and environmental, or C&E, risks, we can only tackle a problem once we get a good grip on its shape and size. Some information may be uncomfortable to face up to – but bringing it to light is the first step in making progress.

When it comes to climate change, the information on what Al Gore famously dubbed an inconvenient truth is indeed getting bleaker by the day.

The most recent IPCC report confirms the dramatic consequences of not taking immediate action: additional global warming of up to 1.5 degrees Celsius in the near term would increase climate hazards, and present numerous risks to ecosystems and human society.

Europe is particularly badly affected, as temperatures here continue to rise above the mean and, despite our efforts to reduce CO2 emissions, we lag far behind in terms of what we need to do to adapt to some of the inevitable consequences.

It is time we face the facts. As citizens, as institutions, and as all actors in the economy – including of course banks.

It is essential that banks share with their stakeholders detailed information on their exposures to C&E – risks. Only then can we all effectively work together to address the consequences of climate change.

This is why today I would like to draw your attention to another important landmark in the ECB's supervision of C&E risks: the publication of our second stocktake on the transparency of banks' disclosures of their C&E risk profiles.

The European and international agenda on climate

Publishing this update is part of our supervisory agenda on climate. As you know, C&E risks have been one of our supervisory priorities for some years now and we have started treating them just like any other prudential risk.

In this context, we have been rolling out a series of corresponding supervisory activities.

In 2020 we published our guide on climate-related and environmental risks, which outlined our supervisory expectations relating to the management and disclosure of C&E risks.

In 2021 we published a self-assessment benchmarking report. And in 2022 we launched the climate risk stress test and a thematic review of how banks incorporate C&E risks into their processes, a fully-fledged supervisory exercise, involving teams responsible for the day-to-day supervision of banks.

At the same time, we are gradually integrating C&E risks into our regular supervisory methodology, and how banks manage these risks will ultimately impact their Pillar 2 capital requirements.

The ECB's supervisory actions on climate are part of broader international efforts to advance the supervision and regulation of C&E risks.

At global level, the Basel Committee on Banking Supervision recently concluded a public consultation on draft supervisory principles for the prudential treatment of climate-related risks, and the input they received is now being reviewed with the aim of finalising those supervisory principles.

This is part of a broader workplan of the Committee to evaluate how to consider climate-related financial risks in all pillars of the Basel framework. Supervision, regulation and – the topic of the ECB report that is published this morning – disclosures.

The importance of transparent disclosures

There is growing international awareness of the great value of transparent disclosures. Disclosures that are clear and easy to understand tend to benefit any company, banks included.

Generally, companies have strong incentives to publish frank and meaningful disclosures because transparency is usually rewarded by investors; it helps reduce uncertainty and allows all interested parties to feel they are making safe investments based on trustworthy data.

This is particularly true for climate-related and environmental risks. As the materiality of physical and transition risks increases by the day, investors are on the lookout for those companies that proactively take these risks into account in their daily operations and across all their activities. One of the essential functions of financial markets is to price risk and thus support informed and efficient capital allocation decisions.

The accurate and timely disclosure of current and past operating and financial results is central to this function. To make it concrete: the more transparent banks are about their C&E risk profiles and their concrete efforts to align their portfolios with the Paris Agreement, the easier it is for market participants to compare banks, reward those which are taking the necessary steps to adopt risk management practices aligned with a carbon-neutral economy, and re-evaluate those with misaligned trajectories.

Transparent disclosures also create a certain level of peer and stakeholder pressure, which is essential to making companies properly manage their risks. Investors and asset managers are seeking to develop and market portfolios that are aligned with the sustainability objectives of their own clients. As such, they are becoming increasingly demanding about corporate C&E disclosures.

Banks' own shareholders are becoming increasingly demanding, too, especially concerning banks that have publicly committed to achieving net zero targets. In fact, failure to disclose meaningful follow-up information on their climate commitments has already led to significant litigation and given rise to heightened reputational and legal risks for some banks.

Recent regulatory and legislative initiatives reflect growing international awareness of the great value of transparent disclosures on C&E risks. In Europe, large banks will have to disclose climate-related information under the European Banking Authority's comprehensive implementing technical standards.

They will have to already do so by early 2023, referencing data from the end of 2022. The information requested from banks includes qualitative and quantitative information on environmental, social and governance risks, as well as indicators such as alignment metrics and the green asset ratio – thus significantly raising the bar in terms of C&E risk reporting.

In the same vein, sustainability reporting obligations under the European Commission's Corporate Sustainability Reporting Directive will shortly apply to large corporations, including banks under our direct supervision.

Main findings of the ECB report on banks' progress towards transparently disclosing their C&E risk profile

The ECB is also well aware of the importance of transparent disclosures. We published our first stocktake of banks' C&E disclosures back in November 2020.

We did so precisely to give banks the time and the incentive to improve the quality of their own disclosures in this field. Back then, virtually none of the institutions in the scope of the assessment met our expectations as set out in the ECB Guide on climate-related and environmental risks, which we published at the same time.

The second stocktake, published today, shows that the quality of banks' disclosures has improved since then, especially in the areas of risk management, governance and business models.

However, this improvement has been only marginal: as of 2021, seven in ten banks disclosed information about C&E risk management and governance – compared to five in ten in 2020 -, while only four in ten shared relevant information about the incorporation of C&E risks into their strategic considerations – up from three in ten in 2020. And, all in all, none of the 115 banks directly supervised by the ECB fully meets our supervisory expectations for disclosures.

There is very little justification for this lack of substantial progress, particularly considering the vast amount and quality of climate-related data, tools and information shared by different international and European organisations and institutions in recent years.

The sheer speed at which regulation and metrics are developing in this field should leave no room for any doubt: addressing climate-related and environmental risks, and publishing good-quality disclosures, is not optional. Banks can and must do much better to improve the quality of their disclosures, and they need to do it quickly.

However, we see a considerable disconnect between banks' perception of the importance of C&E risks as communicated to us, the supervisor, and what banks choose to publicly disclose.

Banks are trying to compensate for the poor quality of their disclosures by issuing a great volume of information around green topics.

We end up with a lot of white noise and no real substance on what both markets and supervisors really want to know: how exposed is a bank to C&E risks and what is it doing to manage that exposure? It is of course relevant for banks to publicise their efforts to, for example, reduce the electricity consumption of their branches.

However, it would be much more significant if they were to announce how they are steering their activities towards risk management practices that are aligned with a carbon-neutral economy. Looking at the world through "green-coloured glasses" is not quite the same as a sound management of all material C&E risks.

We also observe a lack of concrete detail in how banks substantiate their climate-related and environmental metrics and targets. For example, when reporting on their commitment to align with the Paris Agreement, only around one in five institutions disclose the methodologies, definitions and criteria for all of the figures, metrics and targets reported as material.

More than one-third of institutions do not disclose these aspects at all. In light of the increasing importance of such commitments, interested parties will increasingly seek information on these alignment metrics – and banks' disclosures must become meaningful in this regard.

Best practices

Like many other institutions and agencies, the ECB is committed to sharing the best practices we have found across the industry. Not only do they serve as inspiration for banks who need to catch up, they also show that the ECB's expectations can, in fact, be met.

For example, one of the banks under our direct supervision published its own climate strategy – which aims at achieving net zero emissions for its lending portfolio by 2050 or sooner – in tandem with a number of (interim) targets and related metrics, as well as the progress made in meeting them. For each of these targets and metrics, the bank discloses the sectors covered, the underlying methodology and the scenarios used to draw up benchmarks.

For the methodologies and scenarios, it reports on the options it chose, the data sources it used and the changes it made with respect to the previous disclosure.

Another bank endeavoured to align its portfolios with science-based transition pathways, including technology pathways originating from the International Energy Agency's "Net Zero by 2050" report.

The bank disclosed dashboards that displayed the performance of its loan books in various transition sectors, such as power generation, oil and gas, automotive, steel, cement and real estate, against a science-based transition pathway. It also disclosed the precise indicators used, the underlying methodologies and the reference scenarios for each indicator.

For each of the indicators, the bank then disclosed its current and projected performance against the pathway and set associated targets.

Importantly, many of the banks raising the bar in C&E disclosures are small and medium-sized – showing that remarkable progress is achievable by all.

Supervisory follow-up

Let me now outline the next steps that the ECB plans to take to follow up on the results of our assessment of banks' C&E disclosures.

We have sent individual feedback letters to all banks under our direct supervision, setting out the key gaps in their disclosures and conveying our explicit expectation that they will take decisive action to address these gaps. In doing so, banks will ultimately ensure that their risk profile is transparently and comprehensively reflected in the information they disclose to the public. Addressing such gaps will also mean banks are well prepared to meet impending technical requirements.

As I mentioned, the consequences of non-compliance with minimum transparency standards are only going to increase for banks, as legal and reputational risks are starting to materialise for banks which fail to step up the quality of their disclosures.

More and more, clients, investors and other market participants want meaningful, comprehensive information on the climate-related actions of their banks. That way, they can make conscious, informed decisions about where their money goes.

Moreover, failing to disclose exposure to risks, including C&E risks, constitutes a breach of the Capital Requirements Regulation.

As such, we stand ready to use the full array of supervisory tools at our disposal to ensure banks' C&E disclosures are up to our standards, and ultimately that eligible banks are prepared for the new regulatory requirements.

The ECB in addition publishes a yearly report on banks' Pillar 3 disclosures, where we also have the option to publicly list those banks which repeatedly fail to disclose their C&E risks.

In view of the poor results shown by our stocktake, and to assess the extent to which the banks address individual feedback, C&E risk disclosures will continue to feature prominently in the ECB's supervision.

We will assess banks' C&E disclosures again at the end of 2022 and we expect to see major progress by then.

Conclusion

Let me conclude. Stricter disclosure regulation is on the way, and time is running out for banks to get ready. Five years have passed since the Task Force on Climate-related Financial Disclosures published its recommendations. There are also many initiatives, some of them open source, to support banks' efforts.

Many companies have improved their disclosures and now provide information that can feed into banks' own disclosure indicators. And for those banks that have systematically fallen behind the ECB's – and the market's – expectations there is only one way forward. It is time for banks to be transparent and comprehensive with their C&E disclosures, so we that by bringing them to light, we can progress from an inconvenient truth towards a desirable outcome – for us and for all future generations.

Let me end where I started: the first step in coming to grips with any inconvenient truth is full disclosure.

Number 4

Deploying Pseudonymisation Techniques

The case of the Health Sector

As the healthcare domain is attempting to make the most of the evolving technical landscape and adapt the provision of services to fulfil the growing needs of patients in a timely manner, additional cybersecurity and data protection challenges come into play.

The integration of new technologies in already complex IT infrastructures opens up new challenges regarding data protection and cybersecurity.

This is due to the growing need to exchange and share the health related information of individuals among different stakeholders.

It is therefore essential for the entities processing personal data, on the one hand, to collect and further process only data that are necessary for their purposes and, on the other hand, to employ proper organisational and technical measures for the protection of such personal data.

Pseudonymisation is increasingly becoming a key security technique for providing a means that can facilitate personal data processing, while offering strong safeguards for the protection of personal data and thereby safeguarding the rights and freedoms of individuals.

Complementing previous work by ENISA that is relevant, this report demonstrates how pseudonymisation can be deployed in practice to further promote the protection of health data during processing.

Obviously, there is not a single solution on how and when to apply it; in fact different solutions might provide equally good results in specific scenarios, depending on the requirements in terms of protection, utility, scalability, etc.

Pseudonymisation can be a ‘simple’ option to adopt but it can also be comprised of a very complex process, both at technical as well as at organisational levels.

For this reason, defining the goals and objectives of pseudonymisation in each particular case and processing operation is really important.

This report highlights the added value of pseudonymisation in the healthcare sector and demonstrates its applicability through simple but specific use cases.

Complementing relevant ENISA publications in this area, it shows how such techniques can increase the level of protection for personal data being processed in the healthcare domain and will eventually promote and raise awareness on the usability and deployment of such technical measures.

Introduction

Recent decades have witnessed an accelerating pace in the development and adoption of new technologies.

This rapid technological change has also affected the healthcare sector which is going through the digitalisation process and has continuously been adopting new technologies to improve patient care, offer new services focusing on patient-at-home care and even preventive schemes.

The integration of new technologies into already complex IT infrastructures opens up new challenges regarding data protection and cybersecurity as there is an increasing need to exchange and share the health related information of individuals among different stakeholders, in some cases across countries, in order to provide better health services.

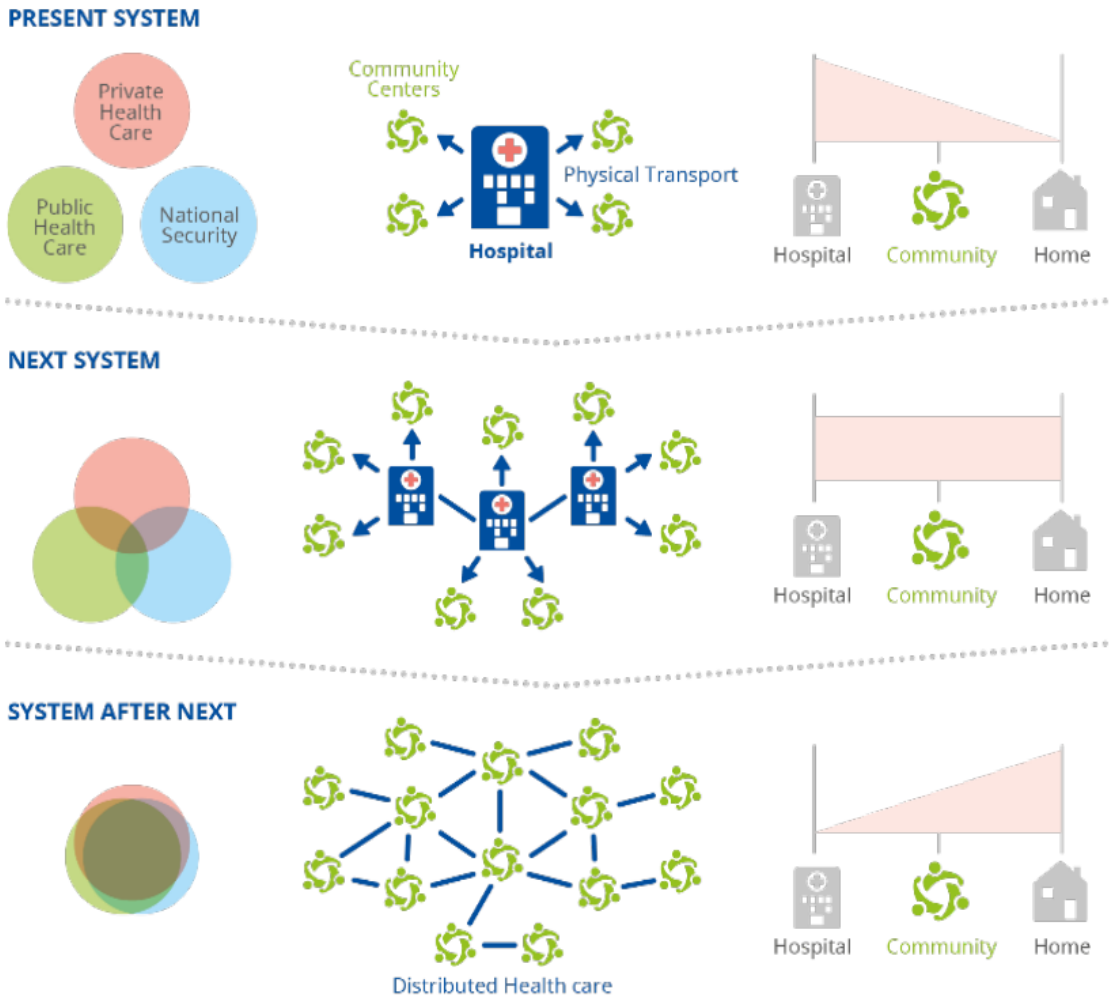
It is therefore essential for the entities processing personal data to collect and further process only data that are necessary for their purposes and, in addition, to employ proper organisational and technical measures for the protection of such data.

Pseudonymisation is one well-known measure that can significantly contribute to this end.

Broadly speaking, pseudonymisation aims at protecting personal data by hiding the identities of individuals in a dataset, e.g. by replacing one or more personal identifiers with the so-called pseudonyms (and appropriately protecting the link between the pseudonyms and the initial identifiers).

This process is not at all new in the design of information systems but gained special attention after the adoption of the General Data Protection Regulation (GDPR), where pseudonymisation is explicitly referred as a technique which can both promote data protection by design (Article 25 GDPR), as well as the security of personal data processing (Article 32 GDPR).

Figure 1: Digital transformation induced shift of value in healthcare [3]



1.1 DIGITAL TRANSFORMATION OF THE HEALTH SECTOR

Health data has always been a valuable source of knowledge in healthcare.

The healthcare domain has historically generated vast amounts of data, both for the treatment of patients and for research and further analysis.

Such processing was mostly performed in paper form but over the last few decades, the accessibility and amount of digitized data has increased massively.

More recently an abundance of new sources of health data occurred as a result of the widespread use of electronic health records, health applications and wearable devices.

Furthermore, advances in computational power have enabled the development of novel data analytics and machine learning techniques that improve diagnostics, treatment and administration in healthcare.

The result is a change in assumptions that is increasingly moving the patient away from hospitalization towards a distributed healthcare system provided by a blend of public and private operators while staying closer to home, as depicted in Figure 1.

To read more:
https://www.enisa.europa.eu/publications/deploying-pseudonymisation-techniques

Number 5

SEC Issues Awards Totaling Approximately $3 Million to Three Whistleblowers

The Securities and Exchange Commission announced three awards totaling approximately $3 million to whistleblowers who provided information and assistance in three separate covered actions.

In the first order, the SEC issued an award of approximately $1.5 million to a whistleblower who provided new information that caused the SEC staff to commence an examination and later open a new investigation into potential securities laws violations. The whistleblower also assisted the staff during the course of the investigation.

In the second order, the SEC awarded a whistleblower more than $1 million for providing information that prompted the opening of an investigation. The whistleblower, an insider who also reported concerns internally, provided continuing assistance to the staff, including multiple interviews.

In the third order, the SEC awarded more than $400,000 to a whistleblower whose comprehensive tip led to an investigation, and thereafter provided substantial ongoing cooperation. The whistleblower also raised concerns internally, causing the conduct to cease.

“Whistleblowers are instrumental to the agency’s ability to detect wrongdoing,” said Creola Kelly, Chief of the SEC’s Office of the Whistleblower. “Each of today’s whistleblowers alerted SEC staff to the securities laws violations and then provided essential assistance that aided the investigation.”

The SEC has awarded approximately $1.2 billion to 254 individuals since issuing its first award in 2012. All payments are made out of an investor protection fund established by Congress that is financed entirely through monetary sanctions paid to the SEC by securities law violators.

No money has been taken or withheld from harmed investors to pay whistleblower awards. Whistleblowers may be eligible for an award when they voluntarily provide the SEC with original, timely, and credible information that leads to a successful enforcement action.

Whistleblower awards can range from 10 percent to 30 percent of the money collected when the monetary sanctions exceed $1 million.

As set forth in the Dodd-Frank Act, the SEC protects the confidentiality of whistleblowers and does not disclose any information that could reveal a whistleblower's identity.

For more information about the whistleblower program and how to report a tip, visit www.sec.gov/whistleblower

Number 6

From open banking to open finance

Denis Beau, First Deputy Governor of the Bank of France, at the France Payments Forum "The Europe of banking and financial services" – Paris

Technological innovations, changes in demand, the arrival of new players: the changes underway in the financial sector are providing a strong impetus to relax the conditions of access to the market, in order to foster competition and thus encourage the development of new, more efficient and less costly services.

In Europe, in the field of payments, this relaxation has already occurred. The EMD, the PSD1 and finally the PSD2 directives have all resulted in the emergence of more agile players, particularly in terms of data exploitation.

The pressure to open up data now extends to insurance and savings: after open banking, we now speak of open finance. This pressure calls for further adapting the regulatory framework. But what should our guiding principles be?

In the payments sector, the main objective of the directives I mentioned was to reconcile openness and security. While this challenge remains relevant for the transition from open banking to open finance, with digitalisation and the development of the platform economy, we have seen two other challenges emerge: reconciling innovation and integration on the one hand and competition and sovereignty on the other.

How do we at the Banque de France and the ACPR, given our role and experience as a supervisor, plan to address these new challenges? This is what I would like to briefly discuss with you today, after a quick recap of the regulatory framework for open banking and the lessons that can be drawn from it to guide the development of open finance.

Part I: Openness and security

A- As regards the assessment of and lessons learned from the regulatory framework for open banking, I would like to start by recalling:

1- The key principles that governed the sharing of payment data: on the one hand, the creation of appropriate statuses and, on the other, the strengthening of security requirements for access.

The creation of the payment service or electronic money service provider status has fostered the emergence of an open banking ecosystem. The introduction of an agent status has also contributed to this process, by creating a gradual – proportionate – regulatory framework: it thus allows emerging players to test the suitability of their services with the market under the aegis of a licensed institution, before applying for a license themselves, if necessary.

2 – These developments have led to the rapid growth of Fintechs, drawing on their competitive advantages: speed, agility and responsiveness to customer needs. The increase in the number of licences and authorisations issued by the ACPR illustrates this success: more than half of the 62 electronic money institutions and payment institutions currently in operation were licensed after 2018; the number of agents registered with the ACPR has risen by more than 40% in one year, with almost 3,300 decisions to register agents in 2021.

3- However, the framework established for open banking has its limitations.

First, in terms of the openness of the market: the new service providers remain dependent on traditional institutions, in particular for the opening of a segregated account, which raises questions given the difficulties that many Fintechs encounter in practice in accessing accounts.

In technical terms too. While the use of APIs makes account access more secure, these interfaces must also ensure that new entrants are able to provide their services at a level of quality that is consistent with their business model, as I will discuss later.

B- As part of our supervisory duties, I can draw two lessons from these observations for the development of open finance regulations: one concerns the statuses that are necessary for the opening of the market, and the other concerns the technical means to ensure proper security.

1- While the creation of new statuses would appear to promote the emergence of new business models, we must nevertheless seek to limit unnecessary sources of complexity and, more fundamentally, the risks of regulatory arbitrage. Here are two examples to illustrate my point.

The first concerns the electronic money and payment service activities and the associated risks, which are now very similar. And yet, there are still differences in their prudential and anti-money laundering frameworks. There are also differences between the competent authorities when it comes to assign innovative payment solutions to regulatory categories.

My second example concerns the draft European MiCA regulation on crypto-asset markets. This draft regulation distinguishes between two kinds of stablecoins: those intended as investment instruments and backed by baskets of assets, Asset-Referenced Tokens (ART), and tokens for payments, Electronic Money Tokens (EMT), whose requirements are similar to those for electronic money.

This distinction requires vigilance in two respects: first, if they are not subject to the same rules, ARTs should not be able to be used for payment purposes; second, care should be taken to ensure that the regulatory requirements are clearly formulated in order to avoid multiple layers of redundant regulation.

2- The second lesson concerns the technical means to be implemented to reconcile openness and security, and in particular the use of APIs.

Should there be an extension of sharing to other financial data, the PSD2 directive calls for a more explicit definition of shareable data, a clearer allocation of responsibilities for authentication, and the promotion of the use of standardised APIs.

Part II: Innovation and integration

A- Let me now turn to the new challenges posed by the development of open banking and its extension towards open finance. I will start with that of promoting innovation without undermining the integration of the European market.

1- In the area of payments, we face a number of challenges, not least that of exchanges between financial intermediaries

The development of the tokenisation of financial assets could lead to a proliferation of new infrastructures that would no longer be interoperable with each other, leading to a risk of market and liquidity fragmentation.

2- This trade-off between innovation and fragmentation risk is also reflected in the settlement asset itself used in payment chains.

If we take the example of stablecoins, their use for the settlement of tokenised financial assets could undermine the stability and efficiency of settlement transactions for new assets by fragmenting the field of settlement assets.

B- To reduce this risk of fragmentation, we have two levers.

1- The first is cooperation between private players to support the efforts of the public authorities to establish a regulatory framework that is clear, proportionate and flexible enough to take account of rapid changes in the market and innovation.

In this respect, there are certainly lessons to be learned from the framework developed for open banking. For example, the deployment of the APIs I mentioned earlier proved to be more complex than expected due to heterogeneous applications, late developments and the lack of an underlying business model.

In this light, two key principles could guide us. On the one hand, institutional players can act as a catalyst for private initiatives on standardisation.

I am referring in particular to the mandate given to the European Payments Council (EPC) for the creation of a dedicated open finance scheme, the SEPA Payment Account Access Scheme (SPAA).

On the other hand, the debate on open finance should also be an opportunity to push for an improvement in the quality of APIs – i.e. premium APIs – by openly addressing the issue of financial compensation for data providers.

2- The second lever is in the hands of central banks, in the form of new services to financial intermediaries.

This is the aim of the Banque de France's experimentation programme with new technologies. These experiments show, in particular, that a wholesale Central Bank Digital Currency (CBDC) would make it possible not only to maintain but also to promote central bank money as the safest and most liquid settlement asset, while adapting it to changes in demand and thus avoiding the fragmentation of settlement assets.

With this improved security, wholesale settlement through distributed ledger could be optimised in terms of efficiency, cost and traceability, including for cross-border payments, by ensuring interoperability between several CBDCs in different jurisdictions.

Part III: Competition and sovereignty

To conclude, I would like to say a few words about the growing challenges related to competition and sovereignty.

A- In this regard, open finance is a development that must be addressed with caution: while it promises to open up the financial market to new players, it could paradoxically increase its concentration, and compromise our strategic autonomy.

1- Indeed, with the platformisation of the digital economy, companies today aim to rapidly increase their market share in a specific segment and then extend the range of their services in order to build a captive customer base.

Open finance could accelerate this trend, which can already be seen in the payments market, by allowing the exchange and cross-referencing of an ever-increasing volume of data.

This may ultimately prove detrimental to competition. This challenge is particularly acute with the development of BigTechs in the financial services markets, which already have significant market power in the areas of cloud computing, mobile payments or digital identification.

2- Open finance also poses challenges in terms of sovereignty to which we must be attentive.

They primarily occur at the individual level. The increasing volume of data in circulation and its cross-referencing is a considerable challenge for the protection of personal data. Cross-border data flows also complicate the enforcement of regulations and make it more difficult for authorities to act.

Secondly, at the industrial level. Mastering artificial intelligence technologies is now contingent on the quantity and quality of accessible data. It is therefore essential that access to data should not be monopolised by non-European players alone.

Lastly, at the State level, because the concentration of data infrastructures raises concerns about their resilience in the event of an attack. Given the geopolitical risks, these aspects should not be underestimated.

The deployment of tokenised settlement assets across borders would also pose a risk to our monetary sovereignty, if it resulted in the use of stablecoins backed by foreign currencies or CBDCs.

B- To reconcile competition and sovereignty, a "retail" central bank digital currency is obviously a potentially important lever.

1- This was the main aim of the investigation phase launched by the Eurosystem in July last year.

Issuing a retail CBDC, nevertheless, raises a number of operational challenges. In particular because financial intermediaries, including banks, play a key role in the security and financial stability of our monetary and financial system.

Introducing a CBDC must therefore neither result in the conversion of a significant proportion of bank deposits into assets held in CBDCs – in normal times as well as in times of stress – nor compete with banks in their day-to-day relations with their customers.

These issues need to be addressed by design in the architecture and functionality of a digital euro, for example by introducing holding limits or by promoting an intermediated model.

This is why it is essential that the financial intermediaries, along with the other stakeholders, be properly involved in the investigation phase that we are conducting: an expert advisory group has already been set up at European level, and this consultation will be extended to all stakeholders in the coming months, in particular via the European and French market bodies at our disposal.

2- But other levers will be needed to reconcile competition and sovereignty.

First and foremost, the regulatory lever. Against this backdrop, we welcome two European texts that are currently being finalised

(i) the Digital Operational Resilience Act (DORA), which aims, among other things, to bring critical service providers under the supervision of financial regulators;

(ii) and the Digital Market Act (DMA), which is intended to ensure that service providers have equal access to the hardware and software components of electronic devices.

These competition and sovereignty concerns should also be taken into account in the revision of PSD2.

Secondly, the industrial lever. While our market is and must remain open, it is nonetheless essential to encourage innovation by European players. This is why, in the area of payments, the Banque de France actively supports the EPI2 initiative for a modern European solution.

In conclusion, we can see that the changes taking place in the financial sector offer the prospect of even more accessible, efficient and innovative

financial services, while at the same time raising new challenges for both market participants and public authorities.

I am convinced that the only way to meet these challenges is through a multi-faceted approach, with cooperation between public and private players.

That is why the Banque de France is fully committed to promoting innovation within a framework of trust: first, at the level of the regulatory framework and as a supervisor, then by facilitating private initiatives and mobilising the market, and lastly, as a driver and player in innovation.

Number 7

Record-breaking, ultrafast devices step to protecting the grid from EMPs

New Sandia diode can shunt excess electricity in a few billionths of a second

Scientists from Sandia National Laboratories have announced a tiny, electronic device that can shunt excess electricity within a few billionths of a second while operating at a record-breaking 6,400 volts — a significant step towards protecting the nation's electric grid from an *electromagnetic pulse*.

The team published the fabrication and testing results of their device on March 10 in the scientific journal IEEE Transactions on Electron Devices. You may visit: https://ieeexplore.ieee.org/document/9732899

The team's ultimate goal is to provide protection from voltage surges, which could lead to months-long power interruptions, with a device that operates at up to 20,000 volts. For comparison, a household electric dryer uses 240 volts of electricity.

An electromagnetic pulse, or EMP, can be caused by natural phenomena, such as solar flares, or human activity, such as a nuclear detonation in the atmosphere. An EMP causes huge voltages in a few billionths of a second, potentially affecting and damaging electronic devices over large swaths of the country.

EMPs are unlikely, said Bob Kaplar, manager of a semiconductor device research group at Sandia, but if one were to occur and damage the huge transformers that form the backbone of our electric grid, it could take months to replace them and re-establish power to the affected portion of the nation.

"The reason why these devices are relevant to protecting the grid from an EMP is not just that they can get to high voltage — other devices can get to high voltage — but that they can respond in a couple billionths of a second," Kaplar said. "While the device is protecting the grid from an EMP, it's at a very high voltage and thousands of amps are going through it, which is a huge amount of power. A material can only handle so much power for a certain amount of time, but we think the material in our diode has some advantages over other materials."

A regulator valve for the grid

The new Sandia device is a diode that can shunt a record-breaking 6,400 volts of electricity within a few billionths of a second — a significant advancement toward being able to protect the nation's electric grid from an EMP. The team, including Sandia electrical engineer Luke Yates, the first author on the paper, is working towards fabricating a diode able to operate at around 20,000 volts, since most grid distribution electronics operate at around 13,000 volts.

Diodes are electronic components found in nearly every electronic device and serve as one-way regulator valves, said Mary Crawford a Sandia Senior Scientist leading diode design and fabrication for the project. Diodes allow electricity to flow in one direction through the device, but not the other. They can be used to convert AC power into DC power, and in this project, divert damaging high voltage away from sensitive grid transformers.

Kaplar agreed that the diode operates somewhat like a regulator valve in plumbing. He said, "In a regulator valve, even if you open that valve all the way, you can't flow an infinite amount of water through the valve. Similarly, there's a limit to how much current you can flow through our diode. If the valve on the pipe is closed, if the pressure reaches a certain point, it'll burst.

Analogously, the diode cannot block an infinite voltage. However, our EMP device uses the point at which the diode can no longer block the high voltage, holds the voltage to that 'pressure,' shunting the excess current through itself, to the ground and away from the grid equipment in a controlled, non-destructive fashion."

The voltage surges caused by EMPs are a hundred times faster than those caused by lightning, so experts don't know if the devices designed to protect the grid against lightning strikes would be effective against an EMP, said Jack Flicker, a Sandia electric grid resiliency expert on the team.

"The electric grid has a number of different protections," Flicker added. "They range in timeframe from very fast to very slow, and they're overlaid on the electric grid to ensure that an event cannot cause a catastrophic outage of the electric grid.

The fastest protection that we typically have on the grid reacts against pulses at one millionth of a second, to protect against lightning. For EMPs, we're talking ten billionths of a second, a hundred times faster."

The new Sandia device can react that quickly.

Growing perfect layers

Part of what makes the diode special is that it is made from gallium nitride, the same basic material used in LEDs, Kaplar said. Gallium nitride is a semiconductor, like silicon. But because of its chemical properties, it can hold off much higher voltage before it breaks down than silicon, Crawford said.

The material itself also responds very quickly and therefore is a good candidate to achieve the fast response needed to protect the grid from an EMP.

Crawford and materials scientists Brendan Gunning and Andrew Allerman made the devices by "growing" gallium nitride semiconductor layers using a process called chemical vapor deposition, she said.

First, they heat a commercially available gallium nitride wafer to around 1,800 degrees Fahrenheit and then add vapors that include gallium and nitrogen atoms. These chemicals form layers of crystalline gallium nitride on the surface of the wafer.

By tweaking the ingredients and the "baking" process, the team could produce layers with different electrical properties. By building up these layers in a specific order, combined with processing steps, such as etching and adding electrical contacts, the team produced devices with the needed behavior.

"A major challenge of achieving these very high voltage diodes is the need to have very thick gallium nitride layers," Crawford said.

"The drift regions of these devices have thicknesses of about 50 microns, or 1/6th of a sheet of notebook paper. This may not sound like a lot, but the growth process we use can have growth rates of only one or two microns per hour. A second major challenge is maintaining very low densities of crystalline defects, specifically impurities or missing atoms in the semiconductor material, throughout the growth time in order to generate devices that work at these very high voltages."

For the team to reach their ultimate goal of a device that operates at 20,000 volts, they will need to grow the thick layer even thicker with even fewer defects, Crawford said. There are several other technical challenges to constructing a device that can operate at such high voltages and currents, she added, including designs to manage the very high internal electric fields within the devices.

Testing ultrafast diodes

Once Crawford's team fabricated the devices, Flicker and his team tested how the devices responded to fast voltage spikes, similar to what would occur during an EMP. His challenge has been modifying a tool to measure the very fast response time of the devices.

"Developing the tools that can accurately measure the very fast responses is very difficult," Flicker said. "If we're talking one or two billionths of a second, they need to be able to measure even faster than that, which is a challenge."

Flicker and his team used very specialized equipment to apply a high voltage pulse, and measure the electric pulse that is reflected back from the diode to tell when the device turns on, very accurately and in less than a billionth of a second.

Useful for smart transformers, solar panel converters and more

Diode devices like the Sandia gallium nitride diode can be used for other purposes, beyond protecting the grid from EMPs, Kaplar said.

These include smart transformers for the grid, electronic devices to convert electricity from roof-top solar panels into power that can be used by household appliances, and even electric car charging infrastructure.

Commonly, solar panel converters and electric car charging infrastructure can handle 1,200 or 1,700 volts, he added. But operating at higher voltage allows for higher efficiencies and lower electricity losses.

Another portion of the project is to develop diodes for these types of devices that operate at high, but not record-breaking voltage but are easier to manufacture, Kaplar said. The Naval Research Laboratory is leading this part of the project.

Some smart transformers and electronic devices can now operate at up to 3,300 volts, Flicker said, but efficiencies would be even greater if they could operate at 10,000 or 15,000 volts with one semiconductor device.

"We have this primary goal of protection of the electrical grid, but these devices have other uses beyond that," Flicker said.

"It's interesting to have our application area, but know that these devices can be used in power electronics, power converters, everything that's at very high voltages."

This research is funded by ARPA-E and the larger project is conducted in partnership with the Naval Research Laboratory, Stanford University, National Institute of Standards and Technology, EDYNX and Sonrisa Research.

You may visit: https://newsreleases.sandia.gov/emp_devices/

Number 8

Consumers warned about chatbot scam

National Cyber Security Centre

Cyber criminals are sending phishing emails inviting people to trace deliveries, only for them to fall victim to a chatbot scam.

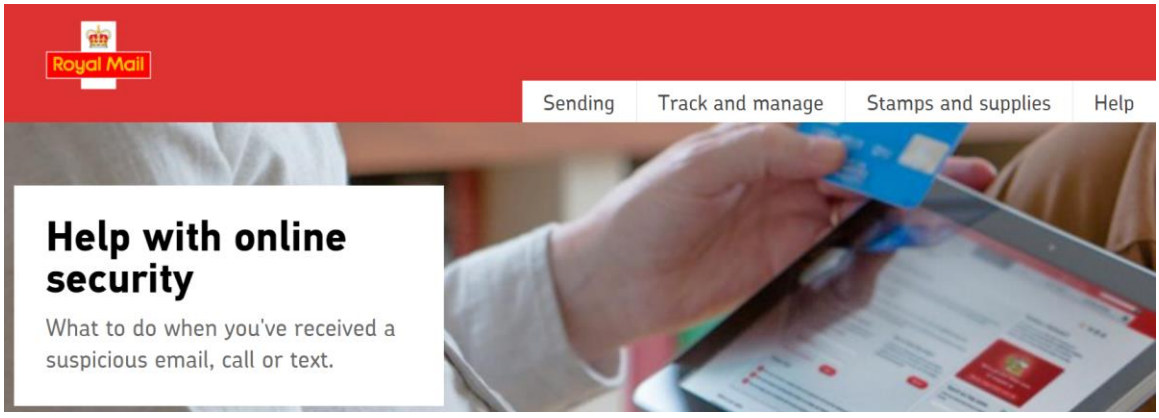
Which? have alerted customers to a chatbot scam which encourages interaction with a service impersonating the Royal Mail. This is the latest evolution to a number of scam communications seen over the past few years that pose as well-known delivery companies. You may visit: https://www.which.co.uk/news/2022/03/watch-out-for-this-royal-mail-chatbot-scam/

Watch out for this Royal Mail chatbot scam

Which? exposes the latest twist on the fake delivery scam

Royal Mail

In the example shown on the Which? YouTube channel, consumers are sent a phishing email which encourages use of the chatbot. The victim will then be given plausible details such as a delivery number before being encouraged to click another link, which takes them to a different website where their name, address and payment details are requested.



The Royal Mail website provides plenty of information on how to check whether something you have seen from them is a scam, and what you can expect from Royal Mail communications. You may visit:
https://www.royalmail.com/help/scam-protection

The NCSC has published guidance on how to protect yourself from phishing scams and how you can report suspicious texts, websites, emails and adverts. You may visit:
https://www.ncsc.gov.uk/collection/phishing-scams

As of February 2022 the NCSC has received over:

10m reported scams

Which has resulted to:

76k scams being removed across 139,000 urls

If you are expecting a delivery and you receive a 'missed parcel' message then don't click the link and use the official website of the delivery company instead.

Number 9

There's More to AI Bias Than Biased Data

Rooting out bias in artificial intelligence will require addressing human and systemic biases as well.

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

As a step toward improving our ability to identify and manage the harmful effects of bias in artificial intelligence (AI) systems, researchers at the National Institute of Standards and Technology (NIST) recommend widening the scope of where we look for the source of these biases — beyond the machine learning processes and data used to train AI software to the broader societal factors that influence how technology is developed.

The recommendation is a core message of a revised NIST publication, Towards a Standard for Identifying and Managing Bias in Artificial Intelligence (NIST Special Publication 1270), which reflects public comments the agency received on its draft version released last summer.

As part of a larger effort to support the development of trustworthy and responsible AI, the document offers guidance connected to the AI Risk Management Framework that NIST is developing.

According to NIST's Reva Schwartz, the main distinction between the draft and final versions of the publication is the new emphasis on how bias manifests itself not only in AI algorithms and the data used to train them, but also in the societal context in which AI systems are used.

"Context is everything," said Schwartz, principal investigator for AI bias and one of the report's authors. "AI systems do not operate in isolation. They help people make decisions that directly affect other people's lives. If we are to develop trustworthy AI systems, we need to consider all the factors that can chip away at the public's trust in AI. Many of these factors go beyond the technology itself to the impacts of the technology, and the comments we received from a wide range of people and organizations emphasized this point."

Bias in AI can harm humans. AI can make decisions that affect whether a person is admitted into a school, authorized for a bank loan or accepted as a rental applicant.

It is relatively common knowledge that AI systems can exhibit biases that stem from their programming and data sources; for example, machine learning software could be trained on a dataset that underrepresents a

particular gender or ethnic group. The revised NIST publication acknowledges that while these computational and statistical sources of bias remain highly important, they do not represent the full picture.

A more complete understanding of bias must take into account human and systemic biases, which figure significantly in the new version.

Systemic biases result from institutions operating in ways that disadvantage certain social groups, such as discriminating against individuals based on their race.

Human biases can relate to how people use data to fill in missing information, such as a person's neighborhood of residence influencing how likely authorities would consider the person to be a crime suspect.

When human, systemic and computational biases combine, they can form a pernicious mixture — especially when explicit guidance is lacking for addressing the risks associated with using AI systems.

To address these issues, the NIST authors make the case for a "socio-technical" approach to mitigating bias in AI. This approach involves a recognition that AI operates in a larger social context — and that purely technically based efforts to solve the problem of bias will come up short.

"Organizations often default to overly technical solutions for AI bias issues," Schwartz said. "But these approaches do not adequately capture the societal impact of AI systems. The expansion of AI into many aspects of public life requires extending our view to consider AI within the larger social system in which it operates."

Socio-technical approaches in AI are an emerging area, Schwartz said, and identifying measurement techniques to take these factors into consideration will require a broad set of disciplines and stakeholders.

"It's important to bring in experts from various fields — not just engineering — and to listen to other organizations and communities about the impact of AI," she said.

NIST is planning a series of public workshops over the next few months aimed at drafting a technical report for addressing AI bias and connecting the report with the AI Risk Management Framework.

For more information and to register, visit the AI RMF workshop page at: https://www.nist.gov/news-events/events/2022/03/building-nist-ai-risk-management-framework-workshop-2

To read more:
https://www.nist.gov/news-events/news/2022/03/theres-more-ai-bias-biased-data-nist-report-highlights

Number 10

Voices from DARPA Podcast Episode 54: Climate Tipping Points

In this episode of the Voices from DARPA podcast, we'll explore a new program with the goal of better identifying and predicting *sudden and catastrophic climate change tipping points*.

Such events could cause major and abrupt disruption to both weather and life on our planet.

DARPA's AI-assisted Climate Tipping-point Modeling (ACTM) program aims to advance artificial intelligence and machine learning to model complex processes that affect Earth's climate, looking for signs of it going disastrously awry.

You'll hear from the program manager and people working on aspects of the problem (from Johns Hopkins Applied Physics Laboratory and the University of Exeter), as well as learn about one especially troubling possibility – the slowing, or even entire collapse, of the Atlantic Ocean's circulating current (with input from Woods Hole Oceanographic Institution).

"DARPA's job is to help the United States avoid strategic surprise," says ACTM program manager Joshua Elliott, "and in my mind there's no bigger risk or strategic surprise than a sudden and massive and irreversible change in some of the key Earth systems that we rely on for survival."

Blubrry (podcast host):
https://blubrry.com/voices_from_darpa/84103686/episode-54-climate-tipping-points

YouTube: https://youtu.be/goOpyrRdda8

iTunes:
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.

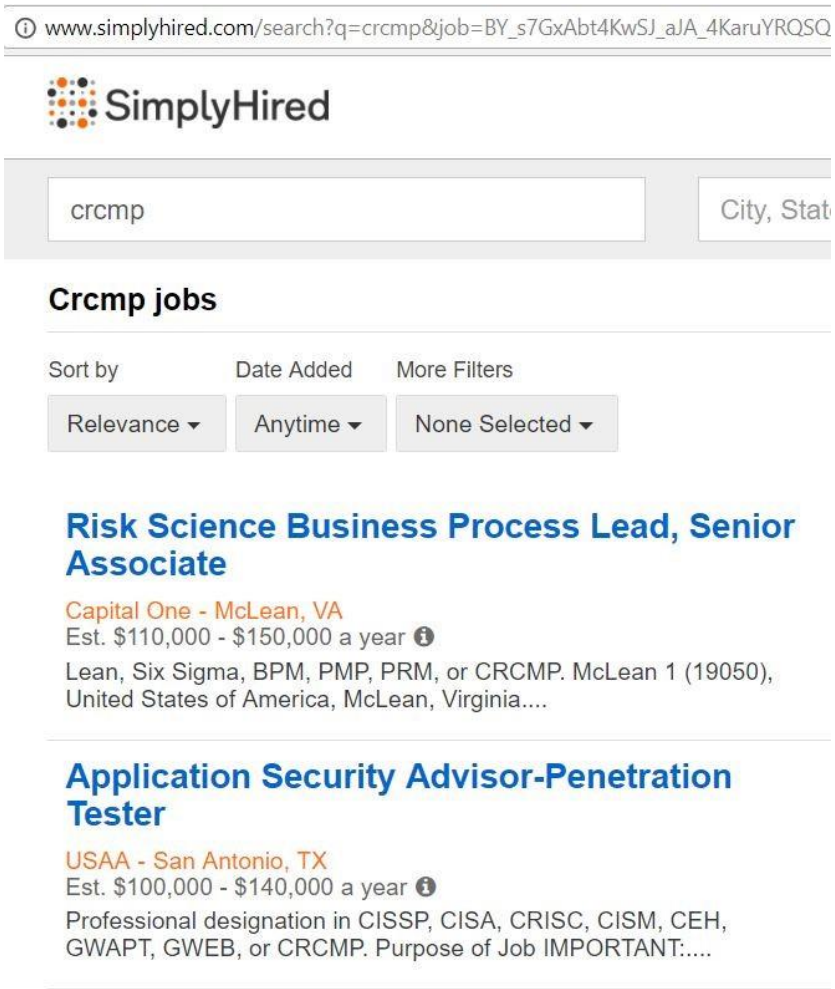
International Association of Risk and Compliance Professionals (IARCP)

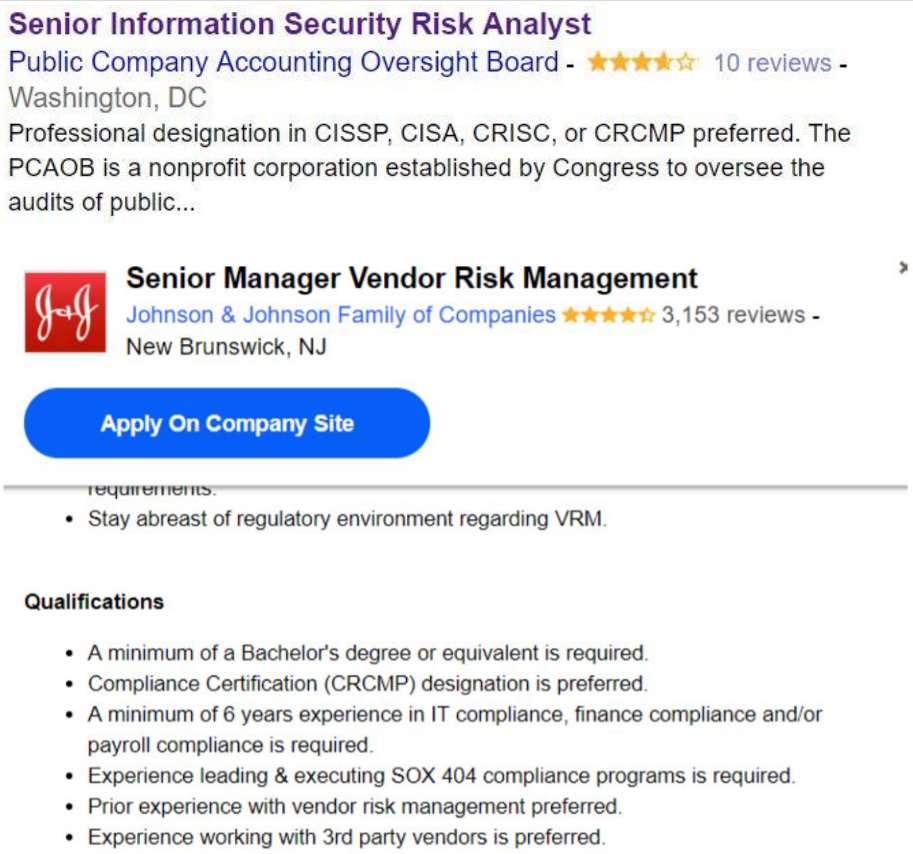
You can explore what we offer to our members:

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





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...

Senior Manager Vendor Risk Management

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

Apply On Company Site

requirements.

- Stay abreast of regulatory environment regarding VRM.

Qualifications

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

Companies and organizations like Accenture, American Express, USAA etc. consider the Certified Risk and Compliance Management Professional (CRCMP) program a preferred certificate. There are CRCMPs in 32 countries.

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

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

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

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

For the Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CRCMP_Re_I.htm
For *instructor-led* training, you may contact us. We can tailor all programs to meet specific requirements.

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