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, May 10, 2021

Top 10 risk and compliance related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next

Dear members and friends,

Nassim Nicholas Taleb has said that *the track record of economists in predicting events is monstrously bad. It is beyond simplification; it is like medieval medicine.*

Today we will speak about *data and medieval architecture.*

If you want to discuss data architecture and the standards that govern which data is collected, how it is stored, arranged, integrated, and put to use in data systems, would you start your presentation with medieval architecture and the great cathedrals of Europe built in the Middle Ages?

Well, Gareth Ramsay, Executive Director for Data and Analytics & Chief Data Officer of the Bank of England did exactly that, and he gave a brilliant presentation. He said:

"The great cathedrals of Europe were built in the Middle Ages by teams of skilled stone masons. To get the dimensions of the building right, it is said that each team would use measures based around the body of the master mason: his foot, his stride, his arm, and so on. And so a local standard was born.

Those standards were designed with one specific use in mind – the construction of that cathedral. And very useful they were, too. But they were closed systems – the foot and the yard used to build one cathedral were different from those used to build another.

And this was not just an English peculiarity: across the channel, a foot length in Strasbourg was 295 mm, a foot in Paris was 325 mm, but a foot in Bordeaux was a relative whopper at 344 mm.

Of course people came to understand the great benefits of enforcing universal, common standards.

In part for maintaining the cathedrals themselves, so that new, replacement stones could be sourced that would fit snugly between their neighbours.

But the benefits of universal measurement standards could be applied a long way beyond the niche discipline of cathedral building.

Now some of you may think that today's financial system is not perfectly comparable to the glorious gothic cathedrals of the Middle Ages.
But like those cathedrals, many of the data systems underpinning today's financial firms and markets were built with narrow reference to their own needs, by their own master masons – their CIOs and systems architects.

They too were closed systems. Each needed to be able to record, track and manipulate its data.

Its data points needed to fit snugly alongside each other. But the design of each system often paid little attention – understandably – to any broader public good.

In this speech, I want to talk about whether there are wider public benefits that might flow from standardising these data labels, and set out a way forward to reap those benefits collectively.

So let me turn from mediaeval architecture to data. At a central bank like the Bank of England, data is our life blood. We depend on our ability to access it, analyse it, and draw conclusions from it to set policies.
Effective management and use of data is how we meet our goals.

Of course, we are far from alone here – many organisations rely heavily on their use of data. But we are, perhaps, different to many in that the vast majority of the data we want is generated by others rather than ourselves. The data we care about is the sum of millions of financial and economic interactions, taking place every second. And much of that data is captured and stored by financial institutions, as they go about serving their customers.

We need to get our hands on that data. We need data on the financial system in aggregate and also on specific markets within it, to help us understand where risks are emerging and to help us calibrate policies to maintain stability. And we need data about individual regulated firms, for our work as supervisor and as resolution authority."

You can read more at number 1 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 1 (Page 6)

From master masons to information architects: how standards can transform reporting (and bring benefits well beyond it)

Gareth Ramsay, Executive Director for Data and Analytics & Chief Data Officer of the Bank of England, webinar hosted by The EDM Council

Number 2 (Page 9)

The Green Swan Conference - Coordinating finance on climate

Bank for International Settlements, Bank of France, International Monetary Fund and Network for Greening the Financial System.

Number 3 (Page 11)

European Cybersecurity Month (ECSM) 2020 Deployment Report

Number 4 (Page 14)

Exploring Research Directions in Cybersecurity

The European Union Agency for Cybersecurity has identified key research directions and innovation topics in cybersecurity to support the efforts of the EU towards a Digital Strategic Autonomy.

Number 5 (Page 16)

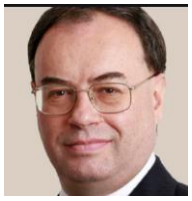
Covid-related fiscal measures and debt sustainability

Prof Claudia Buch, Vice-President of the Deutsche Bundesbank, at the ESM seminar on debt sustainability Panel II "Policy implications in the new normal".

Number 6 (Page 18)

Andrew Bailey: Meeting varied people

Andrew Bailey, Governor of the Bank of England, at Diversity in Market Intelligence: Launching our Meeting Varied People Initiative.



Number 7 (Page 23)

New improvements to Solvency II

BaFin Federal Financial Supervisory Authority

Number 8 (Page 32)

FluBot "package delivery" scam targeting Android devices

National Cyber Security Centre

Number 9 (Page 33)

Emergency Directive 21-03
Mitigate Pulse Connect Secure Product Vulnerabilities

cyber.dhs.gov

Number 10 (Page 38)

Researchers Demonstrate Potential for Zero-Knowledge Proofs in Vulnerability Disclosure

Research teams led by Galois, Trail of Bits develop capability to mathematically prove exploitability of vulnerable software without revealing critical information

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 1

From master masons to information architects: how standards can transform reporting (and bring benefits well beyond it)

Gareth Ramsay, Executive Director for Data and Analytics & Chief Data Officer of the Bank of England, webinar hosted by The EDM Council

Hello all – it's a great pleasure to be speaking to you. I'd like to thank John Bottega and the EDM Council for virtually hosting us today.

I want to begin by talking about cathedrals.

The great cathedrals of Europe were built in the Middle Ages by teams of skilled stone masons.

To get the dimensions of the building right, it is said that each team would use measures based around the body of the master mason: his foot, his stride, his arm, and so on. And so a local standard was born.

Those standards were designed with one specific use in mind – the construction of that cathedral. And very useful they were, too. But they were closed systems – the foot and the yard used to build one cathedral were different from those used to build another.

And this was not just an English peculiarity: across the channel, a foot length in Strasbourg was 295 mm, a foot in Paris was 325 mm, but a foot in Bordeaux was a relative whopper at 344 mm.

Of course people came to understand the great benefits of enforcing universal, common standards.

In part for maintaining the cathedrals themselves, so that new, replacement stones could be sourced that would fit snugly between their neighbours.

But the benefits of universal measurement standards could be applied a long way beyond the niche discipline of cathedral building.

Now some of you may think that today's financial system is not perfectly comparable to the glorious gothic cathedrals of the Middle Ages.

But like those cathedrals, many of the data systems underpinning today's financial firms and markets were built with narrow reference to their own needs, by their own master masons – their CIOs and systems architects.

They too were closed systems. Each needed to be able to record, track and manipulate its data.

Its data points needed to fit snugly alongside each other. But the design of each system often paid little attention – understandably – to any broader public good.

In this speech, I want to talk about whether there are wider public benefits that might flow from standardising these data labels, and set out a way forward to reap those benefits collectively.

So let me turn from mediaeval architecture to data.

At a central bank like the Bank of England, data is our life blood. We depend on our ability to access it, analyse it, and draw conclusions from it to set policies.

Effective management and use of data is how we meet our goals.

Of course, we are far from alone here – many organisations rely heavily on their use of data. But we are, perhaps, different to many in that the vast majority of the data we want is generated by others rather than ourselves.

The data we care about is the sum of millions of financial and economic interactions, taking place every second. And much of that data is captured and stored by financial institutions, as they go about serving their customers.

We need to get our hands on that data. We need data on the financial system in aggregate and also on specific markets within it, to help us understand where risks are emerging and to help us calibrate policies to maintain stability. And we need data about individual regulated firms, for our work as supervisor and as resolution authority.

So we have built data collection processes to give us that data. We publish reporting instructions. Firms then go through various steps: they interpret our instructions, identify the right data within their systems, put in place processes to integrate, cleanse and check the data, and then sign it off and deliver it to us.

But the amount of data we collect through these processes has been growing. It's hard to capture all of our data collections in a single measure. But the accompanying chart shows the number of data points we collect through our regular rule-based banking collections.

Since 2014, this has grown around seven-fold. This growth has partly been a response to the financial crisis of 2008, when regulators and authorities around the world discovered huge gaps in what they knew, and what they could see, of risks emerging in the financial sector.

At the same time, technological change has been increasing the volume of data being produced, and the demands we can put upon the data. Like many of the financial firms we regulate, we want to make more extensive use of this bountiful data, using bigger datasets and newer, more complex analytical techniques.

These developments – the availability of, and need for, more data, and the desire to do more with it – have put growing strains on the processes and systems we use to collect it in the first place. That poses a growing challenge for us and for firms who are sending us the data, each firm doing so independently and in a different way.

And if it's hard for firms to supply us the right data, well, that matters for us. It may take industry longer to meet our requests. And if different firms interpret our requests in different ways, that makes it harder for us to draw conclusions from the data we receive.

To read more:
https://www.bankofengland.co.uk/speech/2021/april/gareth-ramsay-webinar-hosted-by-the-edm-council

Number 2

The Green Swan Conference - Coordinating finance on climate

Bank for International Settlements, Bank of France, International Monetary Fund and Network for Greening the Financial System.

The Bank for International Settlements, Bank of France, International Monetary Fund and Network for Greening the Financial System are joining forces to co-sponsor a truly unique global virtual conference on "How in practice can the financial sector take immediate action against climate change-related risks?".

2–4 June 2021

The 2020 book “The green swan: central banking and financial stability in the age of climate change” (at: https://www.bis.org/publ/othp31.pdf , 115 pages) called for strengthening coordination to address these risks, and for immediate action. Many initiatives by central banks and other actors are already under way – with more under development.

This conference will showcase these initiatives and help to identify more potential practical solutions. Its results can serve as a global public good for other events ahead of COP26, and beyond.

The conference will gather the four heads of the co-sponsoring organisations, three Nobel Laureates, 15+ current and former central bank Governors and top executives, 25+ senior policymakers and official sector experts, 20+ prominent academics and 25+ senior executives and CEOs from the private sector. They will discuss the most feasible and concrete proposals for a more sustainable economy, financial sector and society.

You may visit:
https://www.bis.org/events/green_swan_2021/overview.htm

Number 3

European Cybersecurity Month (ECSM) 2020 Deployment Report

The EU Cybersecurity Act (CSA) came into force on 27 June 2019 with an emphasis on making cybersecurity a priority in awareness campaigns.

In accordance with Articles 4 and 10 of the CSA, the European Union Agency for Cybersecurity (ENISA) must promote a high level of cybersecurity awareness, including cyber hygiene and cyber literacy among citizens, organisations and businesses.

Since 2012, the Agency has been raising public awareness of cybersecurity risks through an annual EU-wide awareness-raising campaign aimed at citizens, organisations and businesses – the European Cybersecurity Month (ECSM).

The month-long campaign every October across Europe, and beyond, promotes cybersecurity awareness and education, and provides guidance on good practices for individuals and organisations in order to create a more cyber secure culture across the EU and increase resilience.

The COVID-19 pandemic changed the scope of the ECSM, but not the level of outreach or success.

Every year, the ECSM has been an interactive month with in-person events spread across countries. It has been a platform for sharing ideas and campaign materials between countries.

The campaign includes new collaboration, workshops, conferences, training sessions and much more.

This year, the pandemic posed a great challenge, namely to transfer this platform to a digital one –for both organisers and participants.

ENISA was up for the challenge. The Agency set forth an ambitious online campaign, entitled 'Think Before U Click', with the social media hashtag #ThinkB4UClick.

The action plan called for an ambassador's programme, a partnership programme and a social media programme.

The online ECSM 2020 campaign was a success, garnering three times more engagement than the previous year.

Each year, the ECSM addresses the disparity between cybersecurity practices across EU Member States.

Number of **activities decrease 20% from 525 to 419**

Number of users who **saw ECSM content increased from 2.7 to 9.8M**

Number of **mentions increased by 265% from 1928 to 7046**

Number of **twitter followers increased by 20% from 20000 to 24000**

Number of **member states collaborating with ENISA** during the campaign **increased by 22%**
(6 more member states actively took part at the campaign, not jut by registering activities)

Number of member states that **gave ECSM a 'good' or 'excellent' rating is up to 78%**

Figure 2: Planning of social media activities

Table 3: Number of #CyberSecMonth campaign mentions per country on a worldwide scale

Most active countries

	COUNTRY	MENTIONS	REACH
1	Italy	281	246 475
2	United Kingdom	215	99 882
3	Norway	137	158 972
4	Spain	91	123 722
5	Romania	85	29 930
6	Greece	60	28 994
7	France	58	63 186
8	Germany	46	129 298
9	Belgium	39	110 723
10	Ireland	38	32 089
11	Iceland	37	32 380
12	Poland	35	2879
13	United States	30	114 174
14	Croatia	29	2724
15	India	28	279 826
16	Slovenia	27	13 397
17	Czech Republic	25	1071
18	Lithuania	21	5534
19	Mexico	20	18 839
20	Bosnia and Herzegovina	19	4032

The report:
https://www.enisa.europa.eu/publications/ecsm-deployment-report-2020

Number 4

Exploring Research Directions in Cybersecurity

The European Union Agency for Cybersecurity has identified key research directions and innovation topics in cybersecurity to support the efforts of the EU towards a Digital Strategic Autonomy.

Resilience, technological sovereignty and leadership are essential for the EU and as such, they are addressed by the new EU Cybersecurity Strategy.

In an effort to support this cybersecurity strategy, the European Union Agency for Cybersecurity releases today a report intended to look into digital strategic autonomy in the EU and suggests future research directions.

What is Digital Strategic Autonomy?

Digital strategic autonomy can be defined as the ability of Europe to source products and services designed to meet the EU's specific needs and values, while avoiding being subject to the influence of the outside world.

In the digital world, such needs may encompass hardware, software or algorithms, manufactured as products and/or services, which should comply with the EU values, and thus preserve a fair digital ecosystem while respecting privacy and digital rights.

To ensure the sourcing of such products and/or services complies with the EU's needs and values, the EU has the option to self-produce them autonomously, or in the case where products and services are acquired from third countries, to certify them and validate their compliance.

However, in cases where there is a high dependence on sourcing, the EU should still be capable of operating its digital infrastructures without giving rise to any possible detrimental influence.

Hence, Europe needs to maintain the capability to produce its critical products and services independently.

In short, digital strategic autonomy means the capacity for the EU to remain autonomous in specific areas of society where digital technologies are used.

Why such a move?

The new challenges brought about by the digitalisation of our environment raise questions on our capacity to retain ownership and control of our personal data, of our technological assets and of our political stand. Such are the main dimensions to be considered under the idea of digital strategic autonomy.

Furthermore, the COVID-19 pandemic highlighted the importance of cybersecurity and the need for the EU to continue to invest in research & development in the digital sector. Within this context, ENISA's report sets and prioritises the key research and innovation directions in cybersecurity.

Key Research Directions: which are they?

The report identifies the following seven key research areas:

1. Data security;
2. Trustworthy software platforms;
3. Cyber threat management and response;
4. Trustworthy hardware platforms;
5. Cryptography;
6. User-centric security practices and tools;
7. Digital communication security.

For each of these areas, the report introduces the current state-of-play in the EU, includes an assessment of current and expected issues. The analyses included serve the purpose of issuing recommendations on cybersecurity related research topics. Such recommendations intend to highlight the bases needed to bolster the EU's digital autonomy.

Who is the report intended for?

Policymakers: the report provides objective-driven strategic guidance on future projects and investments in cybersecurity and can be used for the development of industrial and research policies;

Researchers: the analysis of the areas presented could serve as a guide to address the current research and technological challenges and help to re-assess priorities accordingly.

Further Information:
https://www.enisa.europa.eu/publications/cybersecurity-research-directions-for-the-eu2019s-digital-strategic-autonomy/

Number 5

Covid-related fiscal measures and debt sustainability

Prof Claudia Buch, Vice-President of the Deutsche Bundesbank, at the ESM seminar on debt sustainability Panel II "Policy implications in the new normal".

The pandemic has been a stress test for the global financial system

The coronavirus pandemic has been the biggest stress test for the global financial system in recent decades. It was unexpected, it has been truly global, and it has differed in scale and scope from the global financial crisis in 2008.

In the global financial crisis, excessive leverage in the banking sector led to contagion and a financial crisis that impaired the functioning of the financial system. The coronavirus pandemic, in contrast, threatens the liquidity and solvency of the corporate sector.

So far, the financial system has weathered the storm and continued to function – because policy coordination has worked well during this crisis. Fiscal and monetary policy responses have been bold and timely.

The financial system has proven to be robust: Thanks to the G20 regulatory reforms following the global financial crisis, the banking system is better capitalized, and there is greater regulatory flexibility to reduce pro-cyclicality. Policy responses have been coordinated internationally.

However, key challenges for debt sustainability and financial stability may still lie ahead. Dealing with increasing insolvencies, maintaining crisis-related policy support only as long as necessary, and ensuring financial sector resilience will be among the policy priorities going forward.

There is still a high degree of uncertainty concerning the future evolution of the pandemic and the damage that has been done to the real economy.

One cannot rule out an adverse scenario with feedback loops to the real economy if banks deleverage to meet capital requirements imposed by regulators or markets.

Hence, monitoring the interaction between debt sustainability in the public sector, the corporate sector, and the banking sector will be crucial.

Recognising the importance of fiscal support for financial stability, the European Systemic Risk Board (ESRB) has established a regular monitoring framework.

Since mid-2020, the 30 ESRB Member States have reported the size and uptake of fiscal policy support measures on a quarterly basis (ESRB 2020, 2021). The measures include loan moratoria, public loans and guarantees, direct grants, and tax deferrals, among others.

The reporting has three parts covering the characteristics and volume of measures, their uptake, and qualitative information. Data on characteristics of measures like their announced size, end-dates, or eligibility criteria are made publicly available.

To read more: https://www.bis.org/review/r210423b.pdf

Number 6

Andrew Bailey: Meeting varied people

Andrew Bailey, Governor of the Bank of England, at Diversity in Market Intelligence: Launching our Meeting Varied People Initiative.

Thank you Andrea for that introduction, and thank you to everyone for joining us today.

People often talk about diversity in terms of the makeup of their own workforces – and for a public institution like the Bank, it is vital we reflect the whole society we serve.

This includes both identity and cognitive diversity, which are equally important. I often say I don't want to work in a place that is full of people like me.

I want the Bank to have an inclusive and open culture where people speak up, ensuring we make better decisions by mitigating the risks of groupthink and myopia.

Over recent years, a number of my colleagues at the Bank have also emphasised the importance of diversity and inclusion, both for us as an employer, and as a wider public good for the financial sector.

We have made significant progress internally: for example, launched our Out & Proud Action Plan in September 2020, and continue to sponsor the 'Women in Finance' Charter.

But there is always more to be done, which is why for example we recently initiated a review, led by our Court of Directors, on ethnic diversity and inclusion. I know that many of you are doing similar work within your firms.

As Andrea mentioned, the focus today is our approach to encouraging diversity in our financial market intelligence contacts, and the networks we engage with.

Our priority is to speak to a diverse group of people from a broad range of financial institutions.

Our discussions with market participants help us understand market developments, and the implications for our Policy Committees.

So all of the arguments about why diversity is important internally here at the Bank of England hold just as firmly when we engage with you externally.

We are embedding that approach into our core market intelligence framework, to underscore our commitment.

So why is this a priority for us? First and foremost, it's the right thing to do. As a public institution, we need to represent the diversity of the country in what we look like, who we talk to and the impact of our decisions.

But, just as importantly, it helps us achieve our objectives. Our mission is to promote the good of the people of the United Kingdom by maintaining monetary and financial stability. And diversity in its many forms is a critical part of delivering that mission.

Improved cognitive diversity helps make for better decision making. The lack of such diversity has been highlighted as one important factor in the bank and regulatory failures of 2008.

Having a diverse range of institutions and business models brings positive benefits for financial system resiliency – something that you will not be surprised to hear matters a great deal to the Bank of England!

Diversity in who we speak to in financial markets has even more direct benefits. It improves our understanding of what is driving markets, what people expect from future policy and the potential impacts of different decisions.

And that is critical – because financial markets are global, complex and interconnected.

A failure to understand those diverse components heightens the chances of making analytical, and hence policy, mistakes.

Speaking to only one subset of banks, for example, could mean policy calibrations have unintended consequences for different market participants.

Only looking at established financial assets risks ignoring the impact of innovation. And speaking only to contacts of similar backgrounds could mean missing different perspectives on potential risks to consensus views.

Having that breadth of diverse perspectives allows us to act more quickly and decisively in a crisis too.

In March last year, financial market stress caused by COVID-19 across the world led to investors looking for safe haven assets and cash.

The conversations we had with market participants like you during this period were essential to building a picture of what was happening across a wide range of different markets, and assessing the steps we, and other public authorities, needed to take to maintain economic and financial stability.

To take one example, the intelligence we gathered from you about the stress in the commercial paper market helped the Bank and HM Treasury to plan, design and launch the COVID Corporate Funding Facility in record time, and ensured it was priced appropriately.

Similarly, our market intelligence helped ensure that the other elements of the policy response last year were also rapid, decisive and well calibrated to the underlying risks.

Of course, diversity has affected our other outreach activity too. When I first started working at the Bank of England in the mid-1980s, the Bank's only public statements came mainly from the Governor for instance at the annual Mansion House speech.

We have moved a long way since then, and we see outreach as core to how we operate.

In an important sense this change naturally accompanied the decisive shift to the Bank having clear and independent responsibility for monetary policy and the stability of the financial system.

With those responsibilities went a duty to reach out and communicate much more broadly.

Our network of regional Agents help us with ensuring we speak to companies and organisations from across the country.

We created Citizens Panels – held regularly all over the country in person and, for the time being, virtually – to understand how the public view the economy.
Our Community Forum programme enables us to meet with those who run third-sector organisations, as well as the people they support, across the UK.

Our work in diversity and inclusion extends to our role in creating an inclusive financial sector and I am pleased that with the input of many in the Islamic finance community, we are launching the Alternative Liquidity Facility (ALF) during the course of 2021.

So diversity matters to us. The update of our Market Intelligence Charter and the UK Money Markets Code, published today, will embed diverse outreach into our working practices and help make diversity within financial markets a core standard of best practice.

The Charter sets out our aims and ambitions of talking to a diverse range of contacts and affirms our commitment to open engagement, with an emphasis on challenge and diversity of thought.

The updated Code, which the FCA have recently again recognised as an industry standard, puts the expectation to promote and develop a diverse team upfront, alongside other core principles of best practice, highlighting the benefits of accessing a wider range of skills and thinking.

This approach is also being in embedded in our outward-facing markets committees. We currently have two main committees: the Money Markets Committee and the FX Joint Standing Committee.

We have been working with members from both committees to diversify their membership for some time now: including working to ensure women in senior roles are represented; and that the committees see a wider range of presenters at different stages of the career.

This is yielding results: specifically, female representation – which is one aspect of diversity that has been historically lacking on many senior-level committees – is now approaching half on the UK Money Markets Committee, and has climbed to around a third for the FX Joint Standing Committee in the past 18 months.

These changes were driven by the Bank but importantly with the full support of the external members.

We want to continue to work together with all of you here on this agenda. We look forward to hearing your ideas, suggestions and questions through the panel discussion coming up shortly, and in our networking session with our market intelligence teams later on today.

We want to use that as a starting point to build stronger links with a wider, more diverse group of colleagues, and also deepen those over time, as they progress through their careers.

There is a very important further issue in all of this, which is sadly highly topical, namely to ask what is the antidote to the problem of lobbying? The answer is not to speak to no-one.

That is not likely to lead to good decision making. The answer is to be rigorous about speaking to a diverse range of people to get their views.

We look forward to engaging with you in the future, working together to understand financial market developments from a diverse and varied range of perspectives to inform our policy committee decisions.

Thank you. I am grateful to Christine Boykiw, Sumita Ghosh, Sam Juthani, Ankita Mehta and Arjun Popat for their assistance in helping me prepare these remarks.

Number 7

New improvements to Solvency II

BaFin Federal Financial Supervisory Authority

The European Insurance and Occupational Pensions Authority, EIOPA, has made a number of proposals to the European Commission about how to further improve Solvency II, the European supervisory regime for insurers. This article presents the key points.

Solvency II, the Europe-wide risk-based supervisory regime, has stood the test and should therefore remain in place – this was the provisional appraisal of the European Insurance and Occupational Pensions Authority (EIOPA) at the end of last year.

So, business as usual then? No. In its Opinion on the 2020 review of Solvency II, EIOPA recommends that the European Commission take specific steps to strengthen the supervisory regime in several places.

It was already clear when the framework entered into force at the beginning of 2016 that the effectiveness of its individual elements would be scrutinised after several years.

In a call for advice in February 2019, the European Commission asked EIOPA to issue an opinion, which the industry generally refers to as the Opinion on the 2020 Review. The coronavirus pandemic delayed its release by six months but it is now here in all its complexity.

BaFin has approved the Opinion as a whole. From BaFin's point of view, it was important that the long-term guarantees that are typical in the German insurance industry continue to be possible in the even more market-oriented regime envisaged in the review.

BaFin also argued for reporting to be more risk-based and for the proportionality principle to be implemented more systematically.

The key topics covered in the review also include the national insurance guarantee schemes (IGS) and issues surrounding recovery and resolution, as well as the inclusion of macroeconomic elements in the supervisory framework.

As is typical of a compromise, BaFin managed to achieve some of these goals but had to give ground on others.

Long-term guarantees

Of great significance are the measures for long-term guarantees (LTG) that life insurers, for example, provide to their customers.

One of the objectives of the review was for these guarantees to be incorporated into the provision for long-term contracts in order to more adequately take risks into account, also in view of the low interest rate environment.

In the German market, the most important LTG measures include the extrapolation of the risk-free interest rate term structure, the volatility adjustment and the transitional measures set out in sections 351 and 352 of the German Insurance Supervision Act (Versicherungsaufsichtsgesetz – VAG).

Extrapolating the risk-free interest rate term structure makes it possible to recognise provisions for insurance contracts whose terms extend further into the future than reliable capital market information on risk-free interest rates.

Since sufficient long-term bonds are not available, a last liquid point of 20 years has applied to date – from this point, extrapolation starts, i.e. observable and reliable interest rate data is used to draw conclusions about uncertain interest rates for which there is no reliable data.

The proposed extrapolation method requires insurers to factor in new market information, also beyond the starting point of the extrapolation.

This would increase market consistency and ensure that the interest rate term structure remains stable enough to avoid excessive volatility in the technical provisions and solvency position.

An additional “emergency brake” mechanism is aimed at ensuring that the amount of the provisions remains manageable for undertakings in the industry, even in difficult market situations.

The basis for this mechanism is the situation at the end of 2019. At the time, the net effect was more-or-less balanced in terms of positive and negative effects on capital.

In the case of low interest rates, the mechanism kicks in and limits the adverse effects of the extrapolation, ensuring that there is a balance between positive and negative effects. However, the mechanism is temporary in nature.

At low interest rates, the proposal will therefore place a burden on the capital of German undertakings until final implementation of the new extrapolation method.

The new extrapolation method is a compromise: some representatives of national competent authorities (including BaFin) saw no need for modification, while others advocated a significantly later last liquid point.

The additional capital requirements make it likely that the proposal will give rise to debates in the political negotiations at EU level.

If EIOPA's proposal is approved, the volatility adjustment (VA) will be better aligned with the objectives of the adjustment.

The new VA is aimed at better taking into account the illiquidity characteristics of liabilities and at ensuring a quicker and more efficient response to turbulences on the financial markets.

Those aspects make it simpler to offer long-term guarantees, and BaFin consequently sees their incorporation in the EIOPA Opinion as a success.

EIOPA proposes that insurers better inform professional readers in their solvency and financial condition reports (SFCR) of the transitional measures that they use (see expert article on the BaFin website dated 29 March 2021).

Back in early 2016, the transitional measures were conceived to ease the transition from Solvency I to Solvency II.

And in its current Opinion, EIOPA takes the view that national competent authorities should no longer issue blanket approval of new applications.

For example, if an insurer suddenly finds itself having to rely on the transitional measures five years after Solvency II has entered into force, the national supervisory authority should look into the matter.

In addition to the LTG measures, EIOPA makes further recommendations for Pillar 1, where Solvency II stipulates own funds requirements.

For example, EIOPA proposes to successively reduce future capital requirements within the risk margin to reflect the fact that the probability of recurrence declines once a risk has occurred.

This would significantly reduce the risk margin and thus provide capital relief.

Capital requirements

In BaFin's view, recalibrating interest rate risk is the most important recommendation made by EIOPA with regard to the standard formula that insurers use to calculate their solvency capital requirement (SCR).

This would remedy a technical shortcoming in Solvency II, since the standard formula has so far not taken into account the existence of negative interest rates.

By contrast, the shift approach now proposed maps negative interest rates well, resulting in the actual interest rate risk finally being reflected more appropriately in the SCR. However, this proposal would also impose a burden on undertakings.

The technical proposals that EIOPA has made with the intention of increasing the risk sensitivity of the standard formula comprise recalibrating the market risk correlation between interest rate risk and spread risk, partially recognising retrospective non-proportional reinsurance in non-life reserve risk, and strengthening the effective transfer of risk to reflect risk mitigation techniques.

If EIOPA’s proposal is approved, national competent authorities such as BaFin will require insurers to prepare a finance scheme as soon as they are merely at risk of non-compliance with the Minimum Capital Requirement (MCR).

In this situation, the supervisory authorities will be required to actively examine whether to restrict or prohibit the free disposal of assets.

It must then be stipulated in Level 2 which minimum actions supervisory authorities must take in the event of imminent MCR non-compliance and what the minimum content of the finance scheme must be.

Thresholds and proportionality

To reduce the burden on low risk profile insurers – i.e. mostly small undertakings – EIOPA has pursued two regulatory approaches that BaFin welcomes and supports: thresholds and proportionality.

EIOPA is in favour of increasing the Solvency II exclusion threshold in Article 4 of the Solvency II Directive and proposes a future relevant threshold of EUR 50 million in technical provisions.

It is envisaged that – under certain conditions – Member States will be able to raise the threshold for annual gross written premium income up to a maximum of EUR 25 million.

In Germany, this would likely benefit a notable number of smaller undertakings which would then revert to Solvency I.

Low risk profile insurers are to be allowed to consider as minimum requirements a series of statutory requirements that can be used to apply the proportionality principle.

This would set them apart from medium to high risk profile insurers. Nevertheless, insurers with a higher risk profile are to benefit from the simplified procedures as well, but only with BaFin's consent.

Simplifications in Pillar 1...

Simplifications are to be introduced in all three pillars of Solvency II. In Pillar 1, insurers determine their best estimate, which is an integral part of their technical provisions.

EIOPA intends to reduce the requirements for their stochastic valuation, where permitted by the risk profile. Another proposal is the introduction of a simplified methodology to calculate immaterial risk modules within the standard formula that contribute little to overall risk.

EIOPA also intends to make it easier for low risk profile insurers to perform the stochastic valuation of options and guarantees. Since guarantees also include interest guarantees under life insurance contracts, BaFin considers this recommendation to be inadequate for German life insurers, which are not low risk profile undertakings.

EIOPA also details how insurers should factor the contract boundaries within their portfolios and assumptions about future management actions and expenses into the calculation of their technical provisions.

...and in Pillars 2 and 3

As regards the governance requirements under Pillar 2, many of the new measures are already covered in the Minimum Requirements under Supervisory Law on the System of Governance of Insurance Undertakings (Mindestanforderungen an die Geschäftsorganisation – MaGo).

As a result, the majority of these measures serve merely as clarifications for supervisory practice in Germany.

For instance, EIOPA refers to the opportunity for low risk profile undertakings to combine key functions, to combine key functions with operational functions, or to combine being a key function holder with management board membership.

In Germany, this is already permitted based on the established interpretation. What is also new in Germany is the proposal that insurers with a low risk profile will no longer be required to review their written internal policies on an annual basis but rather every two or three years. Undertakings are to conduct an own risk and solvency assessment (ORSA) only every two years, not annually.

BaFin also supports further Pillar 3 simplifications to be made in the area of reporting. EIOPA recommends introducing risk-based thresholds for quantitative reporting.

In future, undertakings would only submit non-core templates if they exceed the risk-based threshold determined for the reporting template.

The new thresholds would be more tailored to the specific undertaking since they consider the characteristics of the relevant business model more precisely.

The result would be more risk-based and above all less time-consuming submission practices for undertakings.

The solvency and financial condition report (SFCR) and regular supervisory report (RSR) are to be slimmed down and the SFCR is also to be made more suitable for its target audience.

In future, the SFCR is to comprise a two-page summary for policyholders and a more detailed part for professional readers.

Expanded requirements are also planned in specific areas, such as sensitivity analyses for key indicators at undertakings relevant for financial stability purposes.

EIOPA also intends to simplify the supervisory reporting templates; some are to be deleted.

On the other hand, gaps in the reporting package are to be closed, e.g. with EIOPA collecting data on cyber risk with the help of the national competent authorities.

The quantitative reporting requirements for internal models are to be expanded, in some cases significantly. Some deadlines for qualitative and quantitative reporting are to be extended.

Group supervision

Solvency II embodies a supervisory model under which the national competent authority responsible for the ultimate parent undertaking also supervises the group in question.

However, if a subsidiary has its registered office in another EU Member State, the subsidiary is supervised by the local authorities as a solo undertaking. This has occasionally led to inconsistent approaches, which is why EIOPA has taken a closer look at some regulatory areas.

In the past, there have repeatedly been significant differences between Member States with respect to the scope of group supervision. In its Opinion, EIOPA has revised the definition of the term “group” and has developed an overall approach for group supervisors' options not to include individual undertakings in their supervision.

In EIOPA’s view, holding companies must also be included in the SCR and MCR at group level.

If the capital requirements at group level are calculated by combining the accounting consolidation-based method and the deduction and aggregation method, double counting is to be avoided and no material risks are to be overlooked.

As regards the application of partial internal models at group level, EIOPA also recommends demonstrating and documenting the appropriateness of integration techniques more clearly than has previously been required.

To date, the classification of own-fund items at group level has not been uniform across the EU. EIOPA's clarifications work towards ensuring that the requirements are applied consistently.

For instance, groups are to justify the availability of expected profits in future premiums (EPFIPs) at group level.

The generally undisputed inclusion of transitional measures at group level is to be documented in a reconciliation that also calculates the solvency ratio without the benefits at group level.

EIOPA also proposes a specific, uniform method that insurers can use to calculate the minority interests they are required to deduct from consolidated group own funds.

In EIOPA's view, it should be clarified that groups must include in the calculation of group solvency their holdings in companies from other financial sectors with their sectoral own funds or capital requirements.

In relation to governance issues, EIOPA is in favour of removing all room for interpretation and clarifying that the ultimate parent undertaking is responsible for compliance with legal and administrative regulations at group level.

From BaFin's point of view, the proposals are adequate and appropriate to address existing gaps in the regulations and legal uncertainties and to ensure more effective supervision of insurance groups in the EU.

Macro-prudential instruments

To date, Solvency II has only provided for the risk-based solvency supervision of individual insurance undertakings.

EIOPA is now proposing that the macro-prudential perspective be incorporated into the framework in addition to the micro-prudential perspective.

Moreover, national competent authorities are to have the power to set capital add-ons for systemic risk and to prohibit distributions such as dividends.

EIOPA is also proposing that the national competent authorities use the ORSA for macro-prudential purposes and be able to expand their risk and liquidity management requirements to include macro-prudential aspects.

So far, EIOPA has only provided a rough outline of the instruments; in BaFin’s view, these require further development.

The next steps

The Opinion was submitted on 17 December 2020. The European Commission must now address the recommendations and then make its own proposal to the European Council and the European Parliament; this is expected to take place in the third quarter of 2021.

In addition to the requisite modifications to Solvency II, the focus should be on the balance of the package as a whole. This will be followed by trilogue negotiations and it is uncertain how long these will take.

The coming issues of BaFinJournal will address national insurance guarantee schemes (IGS) and the recovery and resolution framework for insurers.

Number 8

FluBot "package delivery" scam targeting Android devices

National Cyber Security Centre

The NCSC is aware that a malicious piece of spyware – known as FluBot – is affecting Android phones and devices across the UK.

The spyware is installed when a victim receives a text message, asking them to install a tracking app due to a 'missed package delivery'.

Scammers and cyber criminals regularly exploit well-known, trusted brands for their own personal gain and the FluBot campaign is a prime example of this.

Android users are urged to familiarise themselves with our guidance and be vigilant to any suspicious-looking text messages, which should be forwarded to 7726. You may visit: https://www.ncsc.gov.uk/guidance/flubot-guidance-for-text-message-scam

If you have already clicked the link to download the application:

You must take the following steps to clean your device, as your passwords and online accounts are now at risk from hackers.

- Do **not** enter your password, or log into any accounts until you have followed the below steps.
- To clean your device, you should:

- Perform a factory reset as soon as possible. The process for doing this will vary based on the device manufacturer and guidance can be found here. Note that if you don't have backups enabled, **you will lose data**.

- When you set up the device after the reset, it may ask you if you want to restore from a backup. You should avoid restoring from any backups created **after** you downloaded the app, **as they will also be infected**.

Number 9

Emergency Directive 21-03
Mitigate Pulse Connect Secure Product Vulnerabilities

cyber.dhs.gov

Section 3553(h) of title 44, U.S. Code, authorizes the Secretary of Homeland Security, in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, to "issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat."

Section 2205(3) of the Homeland Security Act of 2002, as amended, delegates this authority to the Director of the Cybersecurity and Infrastructure Security Agency.

Federal agencies are required to comply with these directives.

These directives do not apply to statutorily-defined "national security systems" nor to systems operated by the Department of Defense or the Intelligence Community.

Background

CISA has observed active exploitation of vulnerabilities in Pulse Connect Secure products, a widely used SSL remote access solution. Successful exploitation of these vulnerabilities could allow an attacker to place webshells on the appliance to gain persistent system access into the appliance operating the vulnerable software. CISA has no knowledge of other affected Pulse Secure products (including the Pulse Secure Access client).

CISA has determined that this exploitation of Pulse Connect Secure products poses an unacceptable risk to Federal Civilian Executive Branch agencies and requires emergency action. This determination is based on the current exploitation of these vulnerabilities by threat actors in external network environments, the likelihood of the vulnerabilities being exploited, the prevalence of the affected software in the federal enterprise, the high

potential for a compromise of agency information systems, and the potential impact of a successful compromise.

CISA has published Activity Alert AA21-110A (https://us-cert.cisa.gov/ncas/alerts/aa-21-110a) providing further details and resources.

Required Actions

By 5 pm Eastern Daylight Time on Friday, April 23, 2021 all federal agencies must:

1. Enumerate all instances of Pulse Connect Secure virtual and hardware appliances hosted by the agency or a third party on the agency's behalf.

2. On every instance of a Pulse Connect Secure appliance identified in the step above, deploy and run the Pulse Connect Secure Integrity Tool (https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB44755)

This tool checks the integrity of the file system and detects any mismatch of hashes. Adversaries are known to maintain persistence over upgrade cycles, and it is critical to run the tool even if all updates have already been deployed and the appliance is running the latest version of software.

Detected mismatched files will be made available for download as an encrypted zip archive.

If an agency's version of Pulse Connect Secure is not supported by the tool, agencies must upgrade the software to the latest version and then run the tool. For a list of supported versions see: https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB44755

a. If the tool does not detect any mismatch of hashes on an initial check, agencies must take one of the following steps until such a time as the vendor releases a patch addressing all of the vulnerabilities covered by this Directive.

i. Continue running the tool every 24 hours, or

ii. Apply a workaround mitigation by importing a vendor-provided XML configuration file (https://kb.pulsesecure.net/pkb_mobile#article/l:en_US/SA44784/s).

b. If the tool detects any hash mismatches or newly detected files:

i. Immediately isolate the appliance from the network while keeping the power on and report the finding as an incident through https://us-cert.cisa.gov/report. The summary details of the scan as reported by the tool must be attached to the ticket.

ii. Immediately create a ticket with the vendor and have them assist with capturing memory and disk forensic images. Due to the vendor's software configuration, CISA cannot assist with the initial forensic capture.

iii. Ensure the forensic artifacts captured in previous steps have been preserved and consult with CISA on further analysis steps.

iv. Affected appliances may be returned into production only after forensic analysis has been completed and remediation requirements from Appendix A have been met.

3. All Pulse Connect Secure appliances in operation must install subsequent updates and security advisories within 48 hours of release by the vendor.

4. Submit a report to CISA using the provided reporting template. Department-level Chief Information Officers (CIOs) or equivalents must submit this report attesting agency status to CISA.

These Required Actions apply to agencies operating Pulse Connect Secure in any information system, including an information system used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information.

Federal Information Systems Hosted in Third-Party Environments (such as Cloud)

CISA is working closely with FedRAMP to coordinate the response to this Directive with FedRAMP Authorized cloud service providers (CSPs).

FedRAMP Authorized CSPs have been informed to coordinate with their agency customers. CISA is also aware of third parties providing services for federal information systems subject to this Directive that may not be covered by a FedRAMP authorization.

Each agency is responsible for inventorying all their information systems hosted in third-party environments (FedRAMP Authorized or otherwise) and contacting service providers directly for status updates pertaining to, and to ensure compliance with, this Directive.

If instances of affected versions have been found in a third-party environment, reporting obligations will vary based on whether the provider is another federal agency or a commercial provider.

If the affected third-party service provider is another federal entity, the provider agency itself is responsible for reporting any incidents to CISA and the customer agency does not have any further reporting obligation.

If the affected third-party service provider is a commercial provider (FedRAMP Authorized or otherwise) and is running an affected version of Pulse Secure (listed above), this is a cybersecurity incident per 44 U.S.C. § 3552(b)(2) and must be reported by the customer agency to CISA through https://us-cert.cisa.gov/report.

All other provisions specified in this Directive remain applicable.

CISA Actions

- CISA will continue to work with our partners to monitor for active exploitation associated with these vulnerabilities.

- CISA will provide technical assistance to agencies without internal capabilities to comply with this Directive.

- CISA will provide updated direction or any additional guidance and indicators of compromise to agencies via the CISA website, through an emergency directive issuance coordination call, and through individual engagements upon request (via CyberDirectives@cisa.dhs.gov). Agencies will be notified of updates via communication from CISA.

- By May 10, 2021, CISA will provide a report to the Secretary of Homeland Security and the Director of the Office of Management and Budget (OMB) identifying cross-agency status and outstanding issues.

Duration

This Emergency Directive remains in effect until all agencies operating Pulse Connect Secure servers have applied forthcoming patches that resolve all currently exploited vulnerabilities or the Directive is terminated through other appropriate action.

Appendix A - Remediation Requirements

After forensic analysis, agencies may proceed with returning the affected appliance into production if the following actions are completed:

a. Save the system and user configuration.

b. Perform a factory reset (https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB22964).

c. Update appliance to the latest version.

d. Re-import the saved configuration.

e. Reset all passwords associated with accounts passing through the Pulse Secure environment (including user accounts, service accounts, administrative accounts and any accounts that could be modified by any account described above). If a Pulse Connect Secure appliance is compromised, all of these accounts should also be assumed to be compromised.

f. Review all configuration settings to ensure no unauthorized changes were made.

g. Deploy and run the Pulse Connect Secure Integrity Tool daily (or implement the XML workaround) until a patch is available.

To read more: https://cyber.dhs.gov/ed/21-03/

Number 10

Researchers Demonstrate Potential for Zero-Knowledge Proofs in Vulnerability Disclosure

Research teams led by Galois, Trail of Bits develop capability to mathematically prove exploitability of vulnerable software without revealing critical information

Today, the disclosure process for software vulnerabilities is fraught with challenges.

Cybersecurity researchers and software security analysts are faced with an ethics versus efficacy dilemma when it comes to reporting or sharing discovered bugs.

Revealing a vulnerability publicly may get the attention of the program's developers and motivate a timely response, but it could also result in a lawsuit against the researcher.

Further, public disclosure could enable bad actors to exploit the discovery before a patch or fix can be applied.

Sharing the vulnerability directly with the software maker on the other hand is ethically sound, but may not necessarily prompt action.

As history has shown, software makers are often reluctant or unwilling to engage with outside security teams and the disclosed vulnerabilities are frequently ignored, or corrective action is dangerously delayed.

DARPA's Securing Information for Encrypted Verification and Evaluation (SIEVE) program is exploring potential solutions to this problem through the use of *zero-knowledge proofs (ZKPs)*.

ZKPs are mathematically verifiable problem statements that can be used to reason about software or systems. The proofs can be used publicly without giving away sensitive information.

SIEVE is focused on developing computer science theory and software capable of increasing the expressivity of problem statements for which ZKPs are constructed while also making it easier to use the cryptographic method.

"Prior to SIEVE, one primary focus of applying ZKP research had been on maximizing the speed of communicating and verifying proofs – sometimes

called 'succinct zero-knowledge'," said Josh Baron, the program manager leading SIEVE.

"For applications like cryptocurrency and blockchain transactions, prioritizing communication and verification efficiency is essential. However, for many potential defense applications, including for highly complex proof statements like those that the Department of Defense may wish to employ, achieving total efficiency and optimization across all metrics may be needed."

In the case of vulnerability disclosure, ZKPs could allow a vulnerability researcher (the prover) to convince a software maker (the verifier) that they possess a piece of information – such as a bug or an exploit – without revealing so much information that their potential for a reward is ruined or requiring that they divulge how the information was uncovered.

One year into the SIEVE program, two research teams have demonstrated the first-ever capability to mathematically prove the exploitability of vulnerable software without revealing critical details around the vulnerability itself or the exploit.

One research team led by Galois, Inc., has demonstrated a ZKP for a previously known memory-safety vulnerability in the Game Boy Advance (GBA) Raster Image Transmogrifier, known as grit.

Memory-safety vulnerabilities are a critical class of vulnerabilities that frequently occur in modern software.

In the Galois-led demonstration, a vulnerability researcher was able to interactively convince another party of the existence of the specific vulnerability in around eight minutes.

To achieve this milestone, researchers developed techniques and prototypes that implement a combination of novel program analyses and protocols for proving and evaluating statements in zero knowledge.

Specifically, the team was able to develop a way to compactly mathematically represent memory-safety vulnerabilities, and then create a zero-knowledge proof based on that representation.

Although the current prototype can only produce proofs for programs that use a restricted set of language features, the Galois team aims to extend its capabilities to prove vulnerabilities of any C/C++ program that can be compiled using a standard compiler.

They are also actively researching prototypes that offer ZKPs of more complex claims, such as a program's overall memory safety.

A second team of researchers from Trail of Bits is working to model vulnerabilities at the systems architectural level, which is a lower level of abstraction than Galois is working on.

Their initial work has created a way to represent real-world instruction set architectures as Boolean circuits – or mathematical models of digital logic circuits – compatible with ZKPs so that users can demonstrate their ability to force a public binary into a specific malicious state.

The team's initial work targets the MSP430 microcontroller, a microprocessor commonly used in embedded systems.

From there, they discovered a way to mathematically represent a variety of common vulnerabilities so that ZKPs could be developed to prove the existence of those vulnerabilities.

The ZKP statement sizes ranged from 86MB to 1.1 GB, and took from 23 seconds to 256 seconds to verify on a desktop PC.

As an example, the team was able to prove that a smart lock using the MSP430 microcontroller could be opened via an undisclosed exploit without having to share details about the exploit or vulnerability.

"Essentially, the researchers took a smart lock, locked it, and then threw away the key. They were then able to exploit the underlying MSP430 to unlock it, and developed a zero-knowledge proof of the exploit to show that it could be done without having to share how it was done," explained Baron.

Trail of Bits has so far demonstrated the ability to perform ZKP disclosure for a wide variety of common types of vulnerabilities in MSP430 binaries, including stack and heap overflows, code injection, format string vulnerabilities, and bypassing memory protections, such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR).

The team is now working to expand the list of supported architectures and runtime environments, with the goal of capturing much of the common x86 architecture.

For example, they plan to produce ZKPs of binaries from DARPA's 2016 Cyber Grand Challenge, which run on DECREE – a simple operating system built on x86.

In this way, SIEVE is building on over a decade of DARPA research in how to formalize cybersecurity.

Disclaimer

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

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

This information:

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

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

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

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

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

- is in no way constitutive of an interpretative document;

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

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

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

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

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

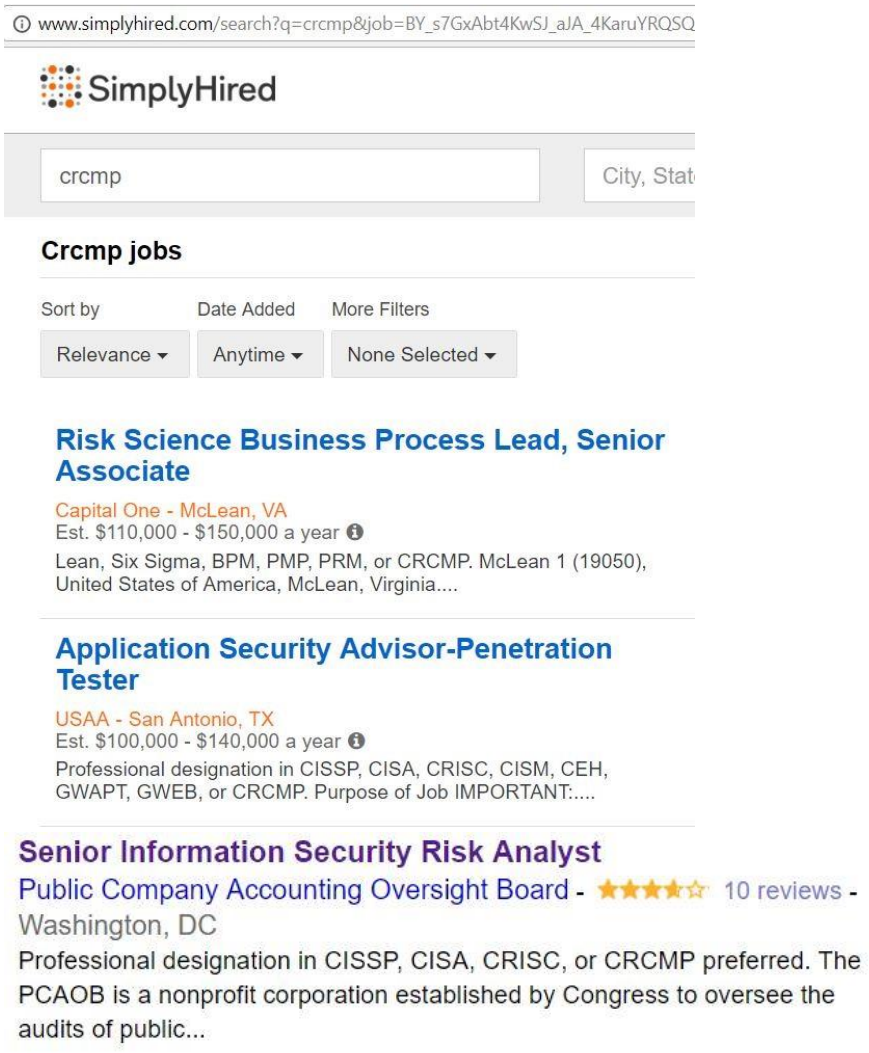
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

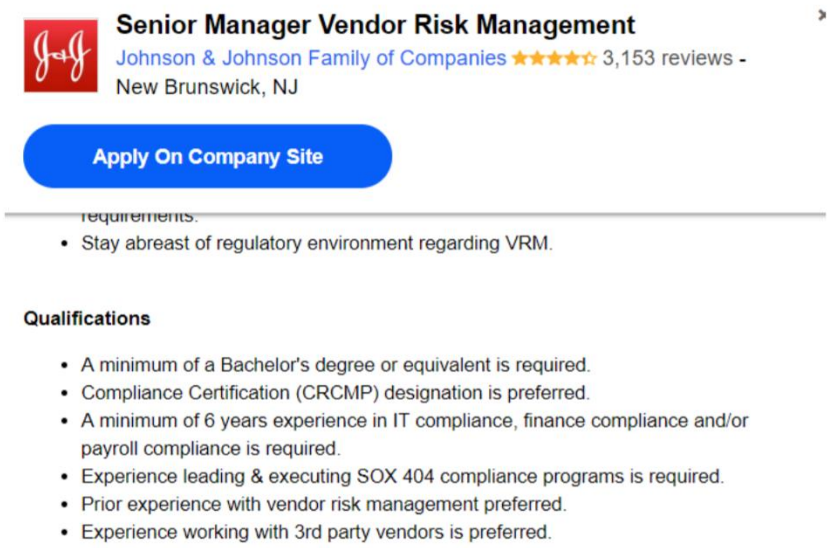
You can explore what we offer to our members:

1. *Membership* – Become a standard, premium or lifetime member.
You may visit:
https://www.risk-compliance-association.com/How_to_become_member.htm

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

3. *Training and Certification* – Become a Certified Risk and Compliance Management Professional (CRCMP), a Certified Information Systems Risk and Compliance Professional (CISRCP), a Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P, and / or a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I.





Senior Manager Vendor Risk Management

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

Apply On Company Site

requirements.

- Stay abreast of regulatory environment regarding VRM.

Qualifications

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

Companies and organizations around the world 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.