Monday, September 28, 2020

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,

Financial interconnectedness can help diversify risk across financial sectors, but can also propagate certain risks during periods of stress.

Interconnectedness has implications for financial stability through funding and credit risk channels, particularly where these channels are associated with the build-up of leverage or maturity/liquidity mismatches.

Therefore, linkages among banks and non-bank financial entities can serve as important *indicators* of potential contagion, within and across borders.

In the wake of the Great Financial Crisis, G20 leaders requested that the Financial Stability Board (FSB) develop recommendations to strengthen the oversight and regulation of “shadow banking”.

The framework developed in response includes the monitoring of non-bank financial intermediation.

Findings are reported annually to provide a global picture of the size and growth of nonbank financial institutions (NBFIs), as well as their links with other parts of the financial system.

Cross-border links between banks and non-bank financial institutions gained momentum in recent years. Banks' cross-border claims on NBFIs rose from $4.6 trillion in Q1 2015 to $7.5 trillion in Q1 2020, a faster increase than that of total cross-border claims.

Financial centres and large advanced economies play a prominent role, as hosts of the largest and most interconnected NBFIs such as central

counterparties, hedge funds and investment funds. The size of banks' cross-border links to NBFIs in emerging market economies has also been on the rise, albeit from a low base.

The financial market turmoil triggered by Covid-19 revealed several vulnerabilities associated with cross-border linkages between banks and NBFIs.

In August, I read the new report from the Financial Stability Board (FSB) with title *Peer Review of Germany*. While the German financial sector remains bank-dominated, the relative importance of nonbanks has increased notably in recent years, and particularly following the global financial crisis.

This increase has been driven mostly by the growth in assets of other financial intermediaries (OFIs), notably investment funds.

The relative importance of NBFI in the German financial system increased between 2002 and 2018 from less than a quarter of total financial assets to over a third (Chart 2).

Chart 2: The financial sector remains bank-dominated but the role of NBFIs has increased

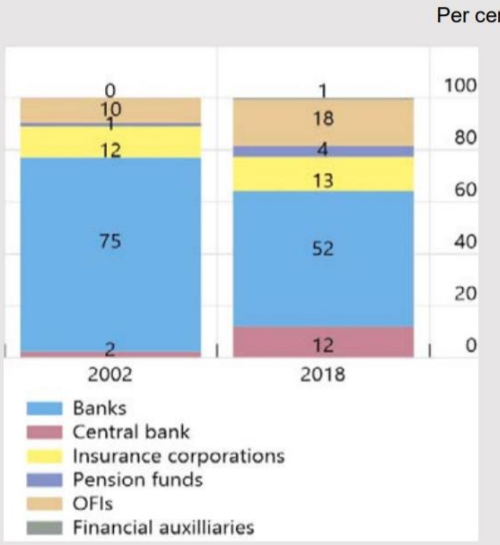
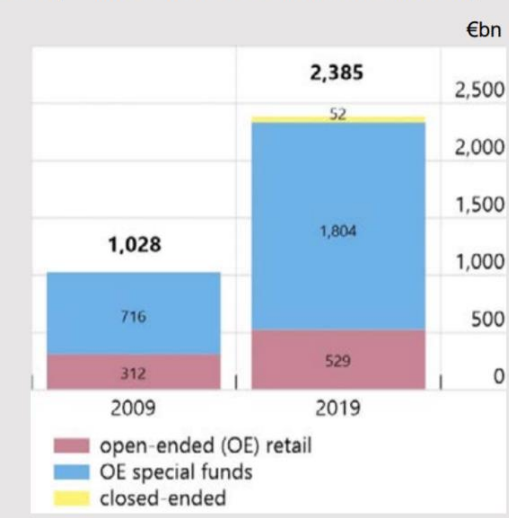


Chart 3: The German fund industry has more than doubled since the crisis, driven by open-end retail funds and special funds



This increase has been driven mostly by growth in assets of OFIs, followed by insurance and pension funds. Investment funds are the largest OFI sub-sector, accounting for over three quarters of OFI assets. According to ECB data, Germany has the third largest fund sector in the Euro Area, with

its €2.4 trillion in assets under management representing 18% of the market.

The industry has more than doubled since the crisis, with the increase driven in particular by open-ended retail and special funds.

Special funds (Spezialfonds) are a type of an alternative investment fund (AIF) that are held mostly by institutional investors. Spezialfonds tend to have only one investor or a limited group of investors (often insurers and pension funds).

This may eliminate the run risk associated with other types of open-ended funds investing in potentially less liquid assets. However, losses in the sector could have an impact on the institutional investor and ultimately on the insurance policy holders or pension policy holders.

Read more at number 3 and 4 below. Welcome to the top 10 list.

Best regards,

George Lekatis

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

BIS

Number 7 (Page 30)

Supervisory action in times of crisis and the limits of the ECB's prudential mandate

Yves Mersch, Member of the Executive Board of the European Central Bank and Vice-Chair of the Supervisory Board of the European Central Bank, at the Eurofi Financial Forum, Berlin.

Number 8 (Page 33)

European Cybersecurity Month: How to Get Involved

October 2020 EU cybersecurity awareness campaign open for event submissions.

enisa
European Network and Information Security Agency

Number 9 (Page 35)

NIST Launches Studies into Masks' Effect on Face Recognition Software

Algorithms created before the pandemic generally perform less accurately with digitally masked faces.

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

Number 10 (Page 38)

DARPA's SIGMA Program Transitions to Protect Major U.S. Metropolitan Region

Advanced radiation detection system operational with Port Authority of New York & New Jersey

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 1

A billion user hours lost in EU telecoms due to security incidents in 2019

The European Union Agency for Cybersecurity publishes the 9th annual report on telecom security incidents.

The report provides an analysis of root causes and impact of major incidents that happened in the course of 2019 and multiannual trends.

The national telecom security authorities in Europe reported a total of 153 major telecom security incidents in 2019.

These incident reports were submitted to the EU Agency for Cybersecurity as part of the annual summary reporting on major telecom security incidents in the EU.

The reported incidents had a total impact of almost 1 Billion user hours lost.

Figure 1: Number of incidents and million user hours lost per year

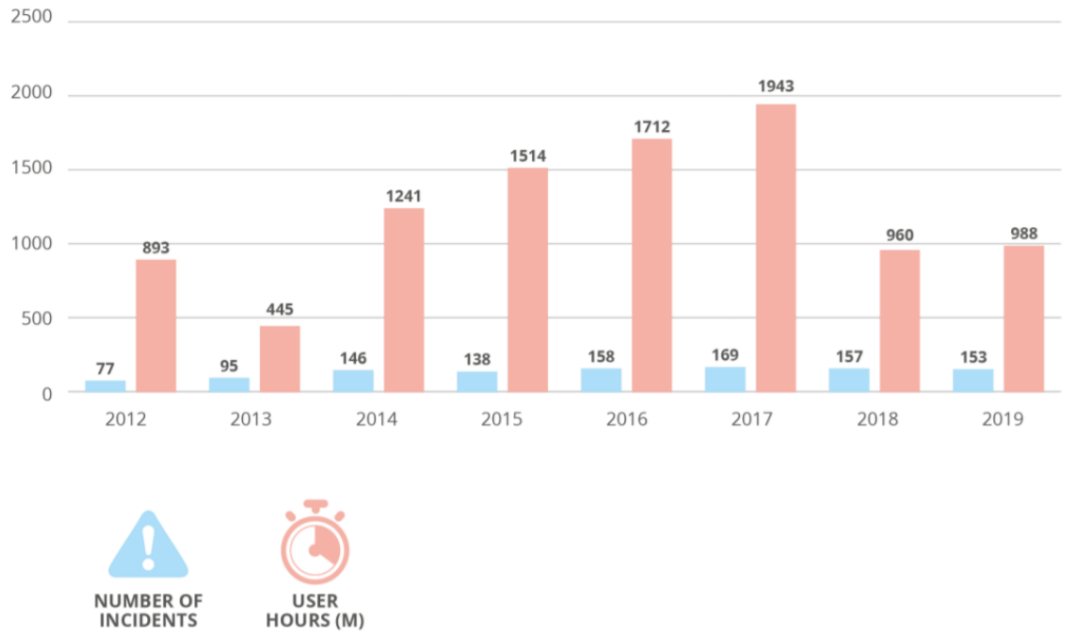
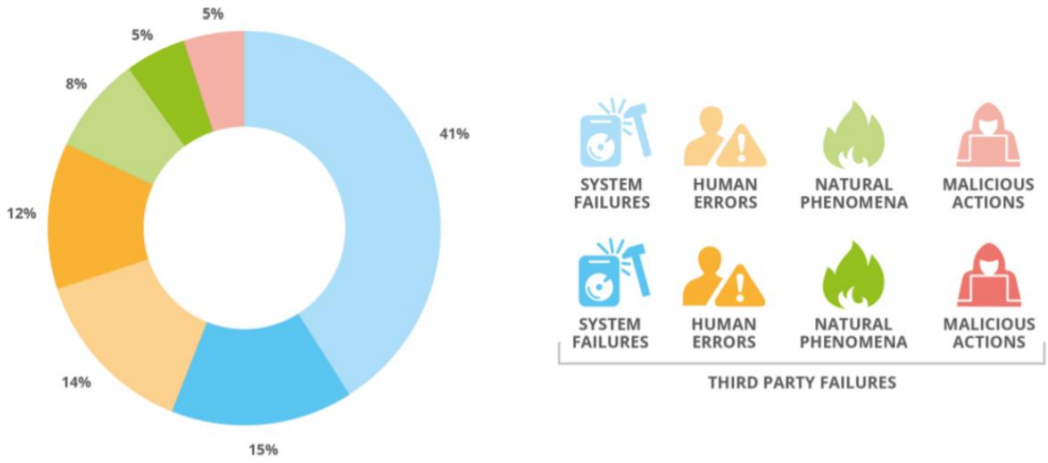


Figure 2: Root Causes and Third party failures – 2019



Key takeaways from the 2019 incidents

- System failures dominate in terms of impact: this category makes up almost half (48%) of the total user hours lost. It is also the most frequent root cause of incidents. Both the frequency and overall impact of system failures have been trending down significantly over the past 4 years;

- More than a quarter (26%) of total incidents have human errors as the root cause. Human errors increased by 50% compared to the previous year;

- Almost a third (32%) of the incidents were also flagged as a third-party failure. This means that these incidents originate at third parties, typically utility companies, contractors, suppliers, etc. This number tripled compared to 2018 when it was 9% then;

- Looking inside the category of system failures, hardware failures are a major factor: almost a quarter of incidents (23%) were caused by hardware failures and they heavily impacted user hours amounting to 38%;

- Power cuts continue to be an important factor: being either the primary or the secondary cause in over a fifth of the major incidents.

EECC broadening the scope of the telecom security incident reporting

The New EU telecom legislation, known as the European Electronic Communications Code (EECC), has to be transposed into national law by 21 December 2020.

These new rules are broader in scope, adapting to the changes in the EU's electronic communications landscape.

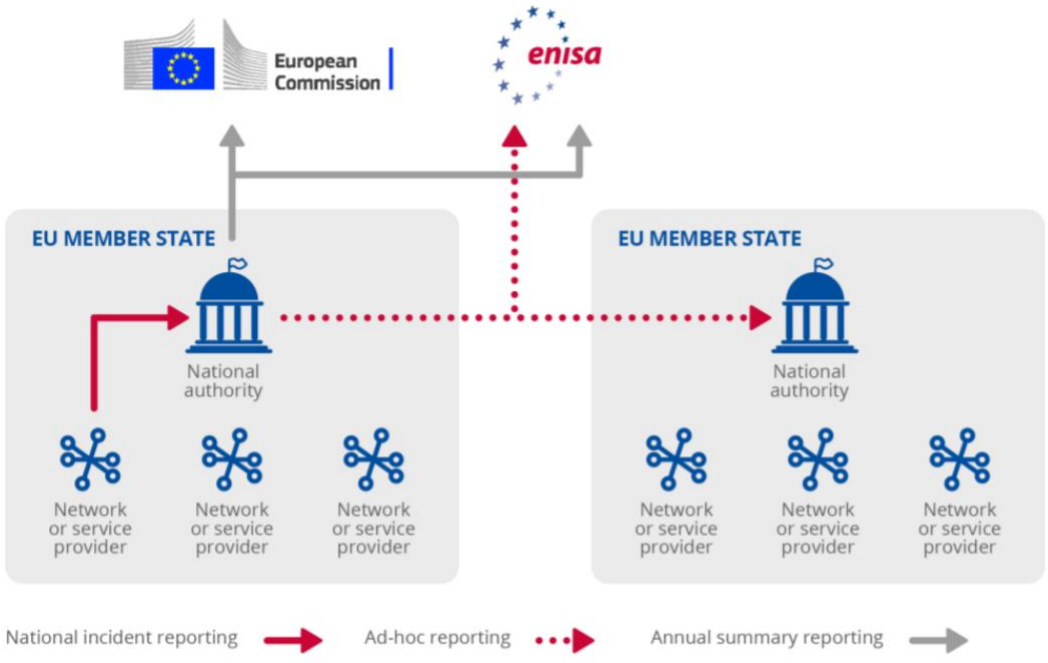
The new legislation will also cover so-called number-independent interpersonal communications services, such as Whatsapp and Skype.

The reporting obligations will cover a broader range of telecom security incidents, including incidents having an impact on confidentiality, availability, integrity or authenticity of the communication networks and the data transmitted via those networks or services.

ENISA is working with the EU Member States to implement these changes. The annual reporting guideline is currently being updated to include new thresholds for the annual summary reporting. The EU Agency for Cybersecurity is also updating the guidelines on security measures.

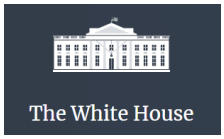
The report:
https://www.enisa.europa.eu/publications/annual-report-telecom-security-incidents-2019

Figure 5: Incident Reporting Framework for Telecom Servicies



Number 2

The Space Policy Directive



Section 1. Background.

The United States considers unfettered freedom to operate in space vital to advancing the security, economic prosperity, and scientific knowledge of the Nation.

Space systems enable key functions such as global communications; positioning, navigation, and timing; scientific observation; exploration; weather monitoring; and multiple vital national security applications.

Therefore, it is essential to protect space systems from cyber incidents in order to prevent disruptions to their ability to provide reliable and efficient contributions to the operations of the Nation's critical infrastructure.

Space systems are reliant on information systems and networks from design conceptualization through launch and flight operations. Further, the transmission of command and control and mission information between space vehicles and ground networks relies on the use of radio-frequency-dependent wireless communication channels. These systems, networks, and channels can be vulnerable to malicious activities that can deny, degrade, or disrupt space operations, or even destroy satellites.

Examples of malicious cyber activities harmful to space operations include spoofing sensor data; corrupting sensor systems; jamming or sending unauthorized commands for guidance and control; injecting malicious code; and conducting denial-of-service attacks.

Consequences of such activities could include loss of mission data; decreased lifespan or capability of space systems or constellations; or the loss of positive control of space vehicles, potentially resulting in collisions that can impair systems or generate harmful orbital debris.

The National Security Strategy of December 2017 states that "[t]he United States must maintain our leadership and freedom of action in space." As the space domain is contested, it is necessary for developers, manufacturers, owners, and operators of space systems to design, build, operate, and

manage them so that they are resilient to cyber incidents and radio-frequency spectrum interference.

Space Policy Directive-3 (SPD-3) of June 18, 2018 (National Space Traffic Management Policy), states that "[s]atellite and constellation owners should participate in a pre-launch certification process" that should consider a number of factors, including encryption of satellite command and control links and data protection measures for ground site operations.

The National Cyber Strategy of September 2018 states that my Administration will enhance efforts to protect our space assets and supporting infrastructure from evolving cyber threats, and will work with industry and international partners to strengthen the cyber resilience of existing and future space systems.

The directive:
https://www.whitehouse.gov/wp-content/uploads/2020/09/2020SPD5.mem_.pdf

Number 3

Cross-border links between banks and non-bank financial institutions

Iñaki Aldasoro, Wenqian Huang, Esti Kemp

BIS

Cross-border links between banks and non-bank financial institutions (NBFIs) gained momentum in recent years.

Banks' cross-border claims on NBFIs rose from $4.6 trillion in Q1 2015 to $7.5 trillion in Q1 2020, a faster increase than that of total cross-border claims.

Financial centres and large advanced economies play a prominent role, as hosts of the largest and most interconnected NBFIs such as central counterparties, hedge funds and investment funds.

The size of banks' cross-border links to NBFIs in emerging market economies has also been on the rise, albeit from a low base.

The financial market turmoil triggered by Covid-19 revealed several vulnerabilities associated with cross-border linkages between banks and NBFIs.

You think that because you understand "one" that you must therefore understand "two" because one and one make two. But you forget that you must understand "and".
Sufi teaching story, as cited in D Meadows, Thinking in systems: a primer

Key takeaways

- Cross-border bank claims on non-bank financial institutions (NBFIs), such as investment funds and central counterparties, have grown 63% in the last five years to $7.5 trillion in Q1 2020.
- Financial links between banks and NBFIs are mainly denominated in US dollars and concentrated in financial centres and large advanced economies, but have also grown in emerging market economies.
- Vulnerabilities stemming from these growing interconnections were highlighted during the Covid-19 market turmoil, for example in fickle dollar funding from NBFIs and liquidity pressures from high central counterparty margins.

Non-bank financial institutions (NBFIs) played an important role in transmitting shocks during the Great Financial Crisis (Gorton (2010),

Claessens et al (2012)). Since then, NBFIs' assets under management have grown substantially, at even a faster pace than banks' (FSB (2020)).

In tandem, national and international authorities have stepped up their efforts to quantify and understand NBFIs' activities and the attendant vulnerabilities (ESRB (2019)).

Of particular concern are links between banks and NBFIs, which, to echo the opening quote, are key "conjunctions" in the financial system.

Both types of institutions can engage in credit, maturity and liquidity transformation, which could underpin the accumulation of imbalances in normal times and pockets of stress in a downturn.

Thus, links between banks and NBFIs are behind particularly powerful transmission mechanisms, as demonstrated most recently by the pandemic-related market turmoil.

This episode underscored that central counterparty (CCP) margins can be procyclical and drain banks' liquidity at an inopportune time; that money market funds (MMFs) can be fickle funding providers to banks; and that banks' positions vis-à-vis NBFIs can contribute to their net long currency positions.

These lessons had an important cross-border dimension. This article is a first attempt at a global mapping of the cross-border links between banks and NBFIs, using the BIS international banking statistics (IBS) and focusing mainly on the residence of counterparties.

We use recent enhancements to these statistics that introduced a more granular breakdown of banks' claims and liabilities vis-à-vis non-banks, in particular NBFIs (Avdjiev et al (2015)).

Since analysis of cross-border links between NBFIs and non-banks is currently hampered by lack of data, we focus on the bank-NBFI nexus.

The rest of the article is organised as follows.

The first section documents the continuous growth of NBFIs as bank counterparties in recent years.

The second presents the network of cross-border links between banks and NBFIs, highlighting the systemic nodes through which shocks could propagate and the growing importance of NBFIs in emerging market economies (EMEs).

The third section assesses vulnerabilities with a particular focus on how they materialised during the Covid-19 fallout in the first quarter of 2020.

To read more: https://www.bis.org/publ/qtrpdf/r_qt2009e.pdf

Number 4

Peer Review of Germany

Review Report

Financial Stability Board (FSB) member jurisdictions have committed, under the FSB Charter and in the FSB Framework for Strengthening Adherence to International Standards, to undergo periodic peer reviews.

To fulfil this responsibility, the FSB has established a regular programme of country and thematic peer reviews of its member jurisdictions.

Country reviews focus on the implementation and effectiveness of regulatory, supervisory or other financial sector policies in a specific FSB jurisdiction.

They examine the steps taken or planned by national/regional authorities to address IMF-World Bank Financial Sector Assessment Program (FSAP) and Reports on the Observance of Standards and Codes recommendations on financial regulation and supervision as well as on institutional and market infrastructure that are deemed most important and relevant to the FSB's core mandate of promoting financial stability.

Country reviews can also focus on regulatory, supervisory or other financial sector policy issues not covered in the FSAP that are timely and topical for the jurisdiction and for the broader FSB membership.

Unlike the FSAP, a peer review does not comprehensively analyse a jurisdiction's financial system structure or policies, or its compliance with international financial standards.

FSB jurisdictions have committed to undergo an FSAP assessment every five years; peer reviews taking place typically two to three years following an FSAP will complement that cycle.

As part of this commitment, Germany volunteered to undergo a peer review in 2019.

This report describes the findings and conclusions of the Germany peer review, including the key elements of the discussion in the FSB's Standing Committee on Standards Implementation (SCSI) in June 2020.

It is the second FSB peer review of Germany, and is based on the objectives

and guidelines for the conduct of peer reviews set forth in the Handbook for FSB Peer Reviews.

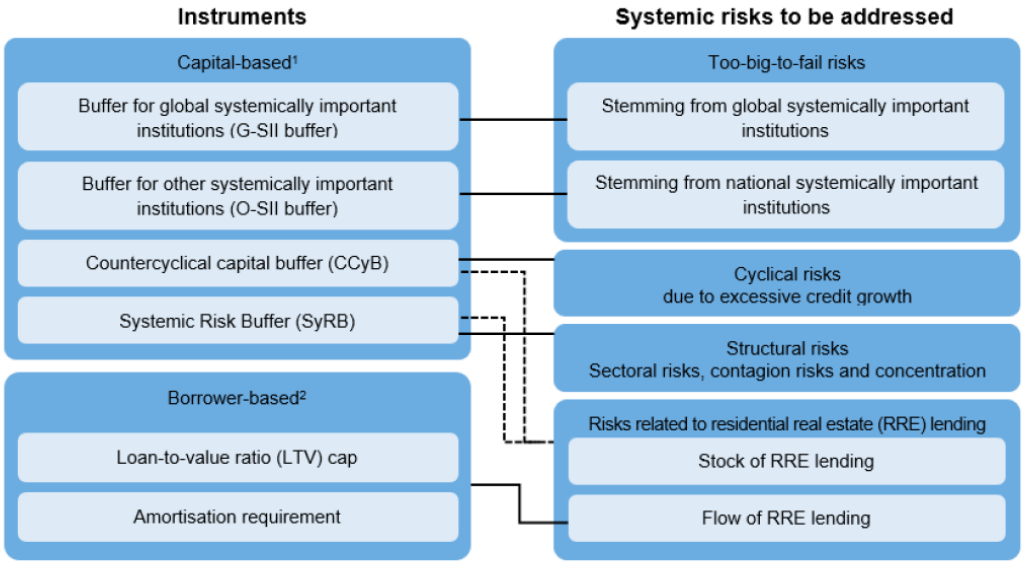
The analysis and conclusions of this peer review are based on the responses to a questionnaire by financial authorities in Germany and reflect information on the progress of relevant reforms as of May 2020.

The review has also benefited from dialogue with the German authorities as well as discussion in the FSB SCSI.

The review process and report preparation largely took place prior to the COVID-19 pandemic; accordingly the report does not examine in depth recent market developments or the related actions by the German authorities.

The draft report for discussion was prepared by a team chaired by Ksenia Yudaeva (Central Bank of the Russian Federation) and comprising Indranil Chakraborty (Reserve Bank of India), Nicoletta Giusto (Companies and Exchange Commission CONSOB, Italy) and Miriam Kurtosiova (Bank of England). Michael Januska and Costas Stephanou (FSB Secretariat) and Maxim Morozov (Central Bank of the Russian Federation) provided support to the team and contributed to the preparation of the report.

Main instruments available to the authorities for macroprudential purposes Figure 1



Source: Bundesbank.[20] Notes: (1) According to EU CRR/CRD IV. Article 458 of the CRR allows for additional measures to address systemic risks such as increased risk weights on real estate lending or a higher capital conservation buffer, or adjustment of public disclosure requirements to reinforce market discipline and improve risk management. (2) Based on national legislation. See Annex 2 for details and additional instruments.

Main findings

Germany's macroprudential framework is well established and operationalised through the Financial Stability Committee (FSC), which adopted and published its macroprudential strategy in 2014.

Data collection, quality and integration have improved, with the FSC facilitating effective information and data exchange across its member authorities: the Bundesbank, the Federal Financial Supervisory Authority (BaFin), and the Federal Ministry of Finance (BMF).

This cooperation in turn has enhanced the FSC's analytical capabilities for the assessment of financial stability risks.

The FSC has further developed its macroprudential toolkit in recent years.

After the FSC recommended in 2015 the introduction of new macroprudential instruments for residential real estate loans, the federal government proposed to establish the legal basis for four borrowerbased instruments.

Subsequently, two borrower-based tools were established by law in 2017, allowing BaFin to set a loan-to-value ratio (LTV) cap and amortisation requirement for new housing loans.

These tools are designed to address potential financial stability risks stemming from developments in the residential real estate market, and they apply to both banks and nonbank financial institutions, but so far have not been activated.

BaFin did, however, activate the countercyclical capital buffer (CCyB) in 2019, in response to an FSC recommendation.

The CCyB rate was subsequently reduced to 0% against the backdrop of the COVID-19 pandemic.

The efforts of the authorities to monitor and manage risks to financial stability from NBFI have increased in recent years as the importance of the sector has grown, most notably with respect to investment funds.

Trends and potential risks relating to NBFI are regularly discussed at the FSC, while BaFin, the Bundesbank and the BMF have established formal and informal structures for coordination and information sharing on NBFI-related matters.

The analytical framework is mainly based on quantitative monitoring, complemented by qualitative information where data gaps persist.

Monitoring of the open-ended investment fund sector in particular has benefited from initiatives to improve data and risk analysis as they relate to funds' credit intermediation, liquidity, leverage and interconnectedness with other sectors.

The authorities have taken steps to increase monitoring of fund liquidity following COVID-19 developments.

BaFin's risk classification methodology for fund managers has been substantially revised and recent legislative changes have extended the set of liquidity management and pricing tools available to asset managers.

To read more: https://www.fsb.org/wp-content/uploads/P270720.pdf

Number 5

Newcastle University suffers a serious cyber incident

National Cyber Security Centre

Newcastle University confirmed that ongoing issues with its IT systems will take several weeks to address. Many of the university's services are not operational and those that are may be taken down without notice.

System issues first started last week and the university has been taking measures to secure its IT estate and investigate the impact since then.

The university has published FAQs which offer advice and guidance to its staff and students.

You may visit: https://www.ncl.ac.uk/itservice/latest-news/faqs/

What is exfiltration?

Exfiltration is an unauthorized data transfer. It occurs when an individual's or company's data is copied, transferred or retrieved from a computer or server without authorization. We have not yet found any evidence of any exfiltration of personal data as a result of this cyber incident.

Is any of my saved work lost?

The University is continuing to investigate the full impact of a cyber incident. It is possible any changes to data made on Saturday 29th and Sunday 30th August will not have been saved so we would advise colleagues to check this.

How long do you estimate it will take to fully restore access to the systems?

Overall, we are making progress with the technical work to assess the full extent of what has happened and to restore full service. As we have said from the start, this is going to take some time to fix and we may have further unexpected disruption to services in the next few weeks.

Will I need to be involved in restoring the system, or will NUIT handle everything?

We will need assistance from system users in some cases and we will make contact (if this is the case) via the Faculty IT managers.

What are the implications for my relationship with external partners?

A statement has been published for our external partners at www.ncl.ac.uk/itservice/latest-news/partners-alumni-updates/

The NCSC is aware of the incident and providing support; we regularly work to protect the academia sector from threats and improve its security practices.

Ransomware operators DoppelPaymer have claimed that they are responsible for breaching the university's network. The university has not confirmed this claim and a criminal investigation is ongoing.

The NCSC has recently updated its guidance on mitigating malware and ransomware attacks.

Those looking to secure their online accounts should follow the NCSC's Cyber Aware advice.

You may visit: https://www.ncsc.gov.uk/cyberaware/home

Anyone concerned about their personal data being compromised may find our guidance on the phishing threat following data breaches helpful.

You may visit: https://www.ncsc.gov.uk/guidance/phishing-threat-following-data-breaches

Number 6

BIS Quarterly Review, September 2020
International banking and financial market developments

Financial markets recorded steady gains during the period under review, after the acute stress in March.

The rebound in valuations was underpinned by supportive monetary and fiscal policy, particularly in some advanced economies (AEs), as well as evidence that the plunge in economic activity had been arrested.

Yet the economic upturn remained incomplete and fragile.

Consensus forecasts indicated that a return to pre-crisis trend growth rates was unlikely.

This raised questions about whether risky asset prices had disconnected from the underlying economic outlook.

There were clear signs of historically high valuations in equity and corporate credit markets.

US and Chinese stock indices extended their April and May gains, surpassing in August the lofty early-year levels.

In other equity markets, the upswing was more moderate.

And the gains were restricted to a limited number of companies.

Amid some recent volatility, technology and health care stocks globally outperformed while energy and financials lagged, possibly reflecting structural changes induced by the pandemic.

In credit markets, spreads narrowed to long-term historical levels, despite evidence of deteriorating credit quality.

Heavy issuance across the rating spectrum, especially in investment grade, though to a considerable extent precautionary in nature, added to the heavily indebted capital structure of many firms.

Central banks largely maintained their policy stance during the period under review.

In late August, the Federal Reserve unveiled its new monetary policy framework, which market participants interpreted as heralding a more prolonged period of accommodation.

Over the review period, interest rate levels and volatility compressed further, providing material support to risky asset prices.

As inflation break-evens returned to pre-pandemic levels, real yields in AEs delved further into negative territory.

In emerging market economies (EMEs), government bond yields retraced the March spike, despite a limited recovery in portfolio inflows.

In this context, a confluence of factors contributed to a depreciation of the US dollar, particularly vis-à-vis AE currencies.

Notably, the rapid fall in US interest rates eroded the yield advantage of dollar assets.

The dollar depreciated most sharply against the euro as market sentiment towards the common currency was buoyed by a more cohesive policymaking environment in the euro area.

Overall, EME currencies remained range-bound, on the back of global investors' lukewarm appetite for local currency assets.

To read more: https://www.bis.org/publ/qtrpdf/r_qt2009.pdf

Number 7

Supervisory action in times of crisis and the limits of the ECB's prudential mandate

Yves Mersch, Member of the Executive Board of the European Central Bank and Vice-Chair of the Supervisory Board of the European Central Bank, at the Eurofi Financial Forum, Berlin.

Today, I will reflect on two issues: our role in the extraordinary measures taken to keep economies afloat since the outbreak of the current crisis, and the limits of the ECB's prudential mandate.

The pandemic has dealt an unprecedented peacetime blow to the European economy. In spring, a great number of our businesses went into full lockdown. Crucially, however, banks in the euro area were able to offer vital support.

To this end, ECB Banking Supervision provided far-reaching capital and operational relief, making record levels of lending possible during this exceptional time.

More precisely, in March we took an unconventional decision: we asked all euro area banks to restrict their dividend distributions.

In July, we extended this recommendation by another three months until the end of this year.

This was not an easy move. Under normal conditions, profitable and healthy banks should not be prevented from remunerating their shareholders.

Restricting dividends can increase banks' funding costs, have an impact on their access to capital markets and make them less competitive than their international peers.

At the same time, I am aware that our recommendation may disproportionately penalise well-capitalised lenders and those set up as non-joint stock companies.

Nevertheless, I still consider such an exceptional and temporary "one-size-fits-all" approach to be warranted.

Our vulnerability analysis only produced accurate estimates of capital depletion on a sector-wide rather than on an individual bank basis.

And, while prudent capital planning is the order of the day, the current economic uncertainty means that banks are simply unable to forecast their medium-term capital needs accurately.

Such an unorthodox move was therefore justified by our ultimate goal to counteract procyclical developments and support banks' capacity to absorb losses during the crisis without compromising their ability to continue lending to the real economy.

Nevertheless, this recommendation is, and must remain, exceptional and temporary.

We will review it in December, and unless we conclude that the banks' capital projections remain clouded by high uncertainty, we will revert to our usual supervisory practice of assessing planned distributions of dividends on a bank-by-bank basis.

We opted to be prudent today to avoid having regrets tomorrow should overall economic conditions further deteriorate.

The ECB is in good company. Other institutions have joined the effort to keep the financial taps open for the real economy during this exceptional period.

After the "quick fix" to the Capital Requirements Regulation, the European Commission recently adopted a Capital Markets Recovery Package to make it easier for capital markets to support the economic recovery.

The proposal to amend the Securitisation Regulation is part of this package. It includes a recital stating that the requirements on direct risk retention, transparency and the resecuritisation ban are also prudential obligations and thus specifically entrusted to the competent authorities in charge of prudential supervision, implying that the ECB has an active supervisory role in these areas. This, in my view, is problematic.

The ECB recognises its competence to supervise banks' adherence to some securitisation obligations that are prudential in nature, such as the use of proper credit granting criteria for exposures to be securitised. However, the

other tasks include the supervision of compliance with direct risk retention requirements, transparency requirements and the ban on resecuritisation.

These tasks fall under the category of product supervision rather than prudential supervision. They ensure the alignment of interests between investors and originators, and between sponsors and original lenders. They allow investors to understand, assess and compare securitisation transactions.

The ECB cannot take on these tasks because they go beyond its prudential supervision mandate. Article 127(6) of the Treaty on the Functioning of the European Union and the SSM Regulation clearly define these limitations. A simple recital cannot change these; only a Treaty change can. Re-labelling financial product supervision tasks as prudential tasks won't do the trick.

What's more, assigning financial product supervision to the ECB could result in conflicting responsibilities. In its role as prudential supervisor, the ECB generally wants as little risk as possible to remain with a bank acting as originator, so as to minimise arbitrage opportunities with the corresponding reduction of capital requirements.

At the same time, the competent authority needs to ensure that the bank retains a material net economic interest under the risk retention obligation. This might be linked to the need to preserve proper credit granting standards but might also create conflict in relation to the ECB's objective as prudential supervisor.

To conclude, I do not see the proposed conferral of tasks as being either a viable allocation of labour or legally tenable. Extraordinary supervisory action is warranted in times of crisis. But the ECB cannot take on tasks that go beyond its prudential supervision mandate.

Number 8

European Cybersecurity Month: How to Get Involved

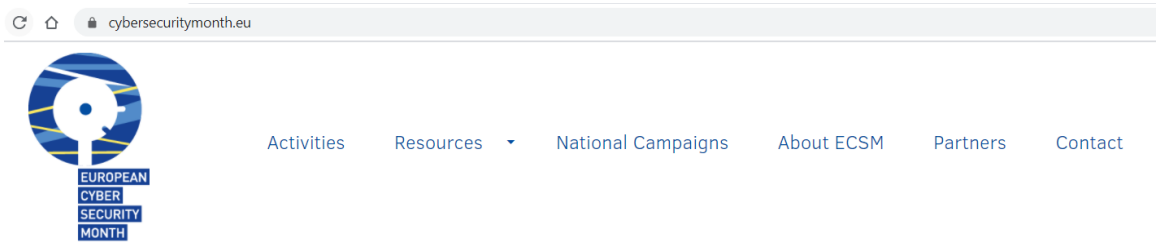
October 2020 EU cybersecurity awareness campaign open for event submissions.

The highly anticipated European Cybersecurity Month (ECSM), the EU's annual campaign in October promoting cybersecurity among citizens and organisations, has opened its doors for people to get involved.

The majority of this year's activities – from conferences and trainings to presentations and knowledge games – have moved online due to the COVID-19 pandemic. Each year, hundreds of activities take place across Europe for the entire month of October to advance online security.

Get Involved

ECSM is an open platform allowing people to join the programme as local event producers. All interested parties can submit their event proposals by visiting the ECSM website (click 'become an organizer'). You may visit: https://cybersecuritymonth.eu/



Accepted proposals will be listed as ECSM activities on the website's interactive map of Europe for public access and registration.

The website acts as a 'hub' of cybersecurity information. Each participating EU Member State has a dedicated webpage with updated information in the local language.

Users can find tips and advice in 23 languages, awareness raising materials, online quizzes, links to events and more.

People can also share their ideas and opinions by joining the cybersecurity awareness campaign on Twitter @CyberSecMonth with #CyberSecMonth and #ThinkB4UClick.

Cybersecurity Is A Shared Responsibility

Each year, ECSM organisers bring together people from across Europe to join forces under the slogan 'Cybersecurity is a Shared Responsibility' to unite against cyber threats.

The ECSM campaign is coordinated by the European Union Agency for Cybersecurity (ENISA) and the European Commission, and supported by the EU Member States and more than 300 partners (governments, universities, think tanks, NGOs, professional associations, private sector businesses) from Europe, and beyond.

Number 9

NIST Launches Studies into Masks' Effect on Face Recognition Software

Algorithms created before the pandemic generally perform less accurately with digitally masked faces.

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

Now that so many of us are covering our faces to help reduce the spread of COVID-19, how well do face recognition algorithms identify people wearing masks? The answer, according to a preliminary study by the National Institute of Standards and Technology (NIST), is with great difficulty.

Even the best of the 89 commercial facial recognition algorithms tested had error rates between 5% and 50% in matching digitally applied face masks with photos of the same person without a mask.

The results were published as a NIST Interagency Report (NISTIR 8311), the first in a planned series from NIST's Face Recognition Vendor Test (FRVT) program on the performance of face recognition algorithms on faces partially covered by protective masks. You may visit: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8311.pdf

"With the arrival of the pandemic, we need to understand how face recognition technology deals with masked faces," said Mei Ngan, a NIST computer scientist and an author of the report. "We have begun by focusing on how an algorithm developed before the pandemic might be affected by subjects wearing face masks. Later this summer, we plan to test the accuracy of algorithms that were intentionally developed with masked faces in mind."

The NIST team explored how well each of the algorithms was able to perform "one-to-one" matching, where a photo is compared with a different photo of the same person. The function is commonly used for verification such as unlocking a smartphone or checking a passport.

The team tested the algorithms on a set of about 6 million photos used in previous FRVT studies. (The team did not test the algorithms' ability to perform "one-to-many" matching, used to determine whether a person in a photo matches any in a database of known images).

The research team digitally applied mask shapes to the original photos and tested the algorithms' performance. Because real-world masks differ, the

team came up with nine mask variants, which included differences in shape, color and nose coverage.

The digital masks were black or a light blue that is approximately the same color as a blue surgical mask. The shapes included round masks that cover the nose and mouth and a larger type as wide as the wearer's face.

These wider masks had high, medium and low variants that covered the nose to different degrees. The team then compared the results to the performance of the algorithms on unmasked faces.

"We can draw a few broad conclusions from the results, but there are caveats," Ngan said. "None of these algorithms were designed to handle face masks, and the masks we used are digital creations, not the real thing."

If these limitations are kept firmly in mind, Ngan said, the study provides a few general lessons when comparing the performance of the tested algorithms on masked faces versus unmasked ones.

1. Algorithm accuracy with masked faces declined substantially across the board. Using unmasked images, the most accurate algorithms fail to authenticate a person about 0.3% of the time.

Masked images raised even these top algorithms' failure rate to about 5%, while many otherwise competent algorithms failed between 20% to 50% of the time.

2. Masked images more frequently caused algorithms to be unable to process a face, technically termed "failure to enroll or template" (FTE).

Face recognition algorithms typically work by measuring a face's features — their size and distance from one another, for example — and then comparing these measurements to those from another photo.

An FTE means the algorithm could not extract a face's features well enough to make an effective comparison in the first place.

3. The more of the nose a mask covers, the lower the algorithm's accuracy. The study explored three levels of nose coverage — low, medium and high — finding that accuracy degrades with greater nose coverage.

4. While false negatives increased, false positives remained stable or modestly declined. Errors in face recognition can take the form of either a "false negative," where the algorithm fails to match two photos of the same person, or a "false positive," where it incorrectly indicates a match between

photos of two different people. The modest decline in false positive rates show that occlusion with masks does not undermine this aspect of security.

5. The shape and color of a mask matters. Algorithm error rates were generally lower with round masks. Black masks also degraded algorithm performance in comparison to surgical blue ones, though because of time and resource constraints the team was not able to test the effect of color completely.

The report, Ongoing Face Recognition Vendor Test (FRVT) Part 6A: Face recognition accuracy with face masks using pre-COVID-19 algorithms, offers details of each algorithm's performance, and the team has posted additional information online. You may visit: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8311.pdf

NISTIR 8311

Ongoing Face Recognition Vendor Test (FRVT)

Part 6A: Face recognition accuracy with masks using pre-COVID-19 algorithms

Ngan said the next round, planned for later this summer, will test algorithms created with face masks in mind. Future study rounds will test one-to-many searches and add other variations designed to broaden the results further.

"With respect to accuracy with face masks, we expect the technology to continue to improve," she said. "But the data we've taken so far underscores one of the ideas common to previous FRVT tests: Individual algorithms perform differently. Users should get to know the algorithm they are using thoroughly and test its performance in their own work environment."

This work was conducted in collaboration with the Department of Homeland Security's Science and Technology Directorate, Office of Biometric Identity Management, and Customs and Border Protection.

Number 10

DARPA's SIGMA Program Transitions to Protect Major U.S. Metropolitan Region

Advanced radiation detection system operational with Port Authority of New York & New Jersey

On a blustery winter day last December, a car carrying radioactive material approached one of the Port Authority of New York and New Jersey's major transportation hubs.

As the car got closer, an alarm flashed and sounded on a large monitor in the police operations center, identifying on a digital map the exact location of the vehicle and the specific radioactive isotope radiating from the car – Cesium-137.

Within minutes, officers in the Port Authority Police Department – equipped with vehicle-mounted and pocket-sized radiation sensors displaying the same real-time digital map – tracked the vehicle and apprehended the suspects in a parking lot.

Thankfully, the potential terrorists and radiation-emitting isotope were not a threat, as the scenario was only a drill.

The December exercise marked the capstone for DARPA's SIGMA program, culminating a five-year effort to develop and deploy an automated, high-performance, networked radiation detection capability for counterterrorism and continuous city-to-region scale radiological and nuclear threat monitoring.

The transition of the radiation-detection system took place prior to the coronavirus disease (COVID-19) pandemic. In the eight months since the SIGMA transition, DARPA has been developing and testing additional sensors under its SIGMA+ effort to detect chemical, biological and explosive threats as well.

"We want to thank the Port Authority for their outstanding support throughout the SIGMA program and their continued support as we test SIGMA+ sensors," said Mark Wrobel, DARPA program manager in the Defense Sciences Office. "Being able to test and refine the system in the country's largest metropolitan region was invaluable in taking SIGMA from a research project to an operationally deployed system in just five years."

SIGMA adds an additional layer of radiation-detection capability for the Port Authority.

“New York City and Northern New Jersey have some of the nation’s most critical transportation infrastructure – heavily trafficked tunnels, bridges, airports, train and bus stations, and ferry terminals,” said Dave Warrington, senior manager for strategic preparedness in the Port Authority’s Office of Emergency Management.

“This unique partnership with DARPA was mutually beneficial – DARPA had access to our transportation nodes to collect real background radiological data for developing the system, and the Port Authority now has a network of high-performance stationary, vehicle-mounted, and wearable sensors providing enhanced, 24-hour nuclear and radiological threat detection.”

Port Authority Police Department (PAPD) officers commented on the capabilities and improved detection sensitivity SIGMA provides, significantly reducing false-positives.

“Our legacy radiation-detection system takes a lot more time to identify if a radioactive hit is a threat or a non-threatening source, such as construction-site materials,” said Lt. Rich Munnelly, emergency management liaison officer at PAPD headquarters.

“SIGMA enables much faster reaction time, since you don’t need to wait for additional equipment to be brought in to evaluate the radioactive material. With SIGMA, the first responder knows immediately via handheld display what the radioactive isotope is and can quickly determine if it’s a threat or not.”

Munnelly noted how user friendly the system is. SIGMA uses an app-like Android interface that is easy to train new officers on.

He also highlighted how the network allows officials up the chain of command to follow alerts and track potential threats in real-time along with first responders, significantly streamlining the coordination process across various levels of command and with federal agencies in the case of a radiological event.

“The system automatically sends officers alert notifications and texts, which is key,” Munnelly said. “Everyone gets all the information at the same time, and because the various sensors are networked it allows for remote monitoring and standoff detection, increasing safety for our officers and the public.”

Another benefit of the SIGMA sensors is their reduced size, weight, and power – from the portable sensors first responders wear on their vest to the more powerful sensors carried in police vehicles, to the stationary sensors at key transportation nodes.

For example, legacy vehicle-borne sensor packages take up the whole vehicle, Warrington said, whereas SIGMA's vehicle-mounted detectors require significantly less space, allowing vehicles to perform their primary function and have room for additional gear.

Most importantly, SIGMA runs continuously, analyzing background radiological conditions daily to constantly refine threat-detection algorithms.

"It's not a closed-end system," Munnelly said. "Software refreshes are pushed out regularly, updating isotope profiles to improve detection of known threats and to account for potential new ones."

The use of this constantly collected background data also supports reduction in false and nuisance alarm rates, a major operational burden with legacy systems.

The DARPA performers who developed the SIGMA radiation detectors and network are Physical Sciences Inc., Kromek Ltd., Silverside Detectors, and Two Six Labs.

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.

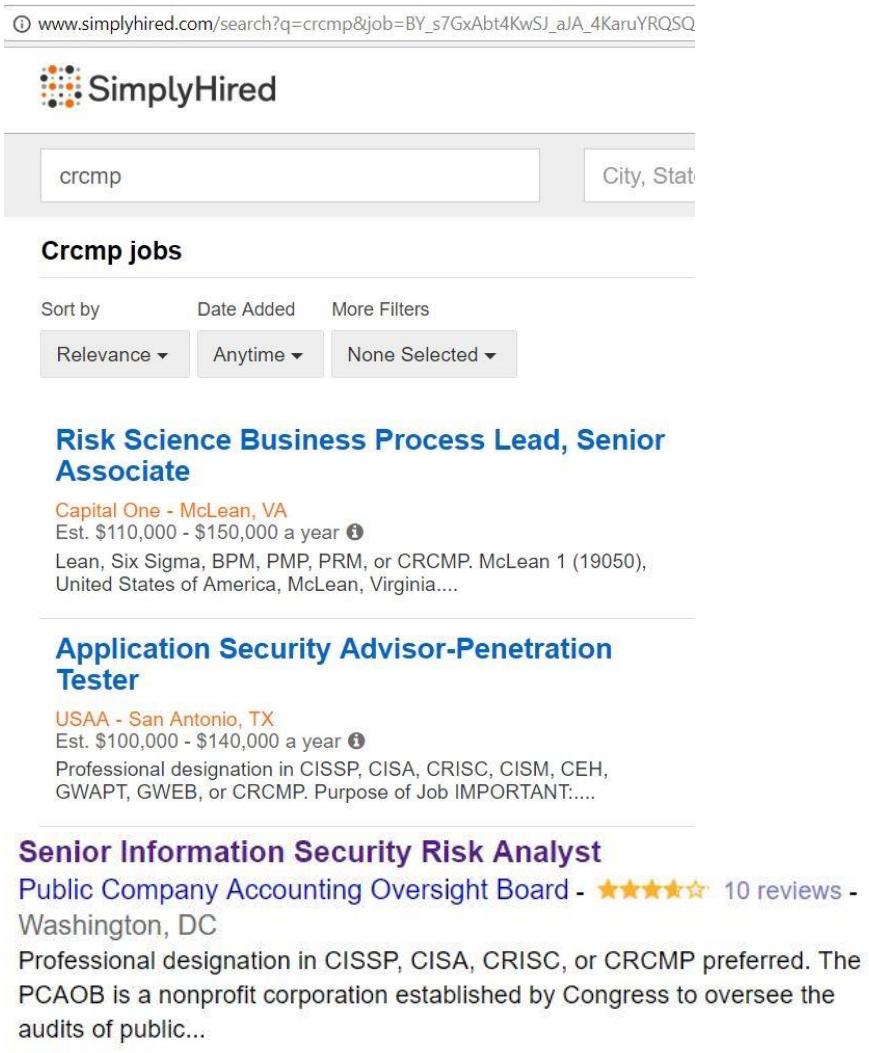
International Association of Risk and Compliance Professionals

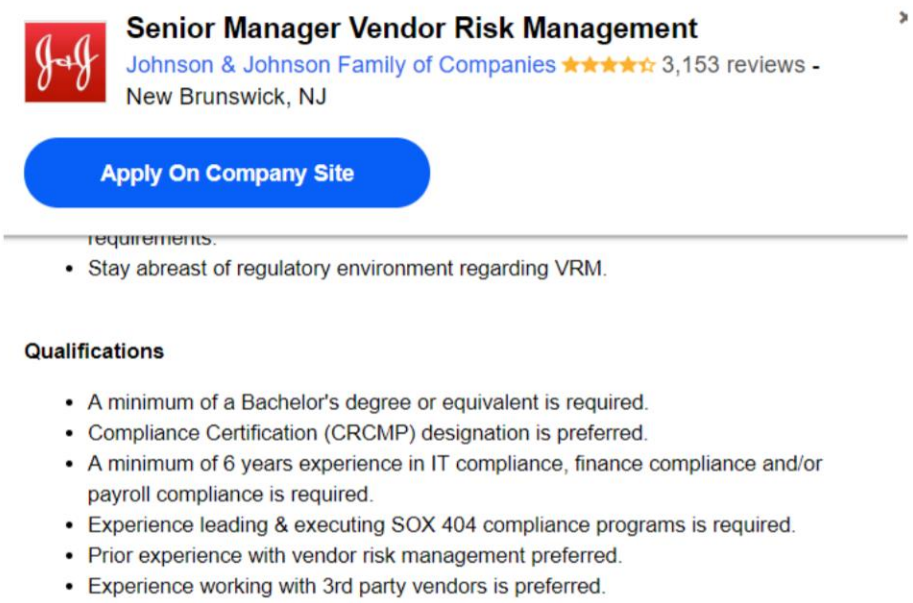
You can explore what we offer to our members:

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

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

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





Senior Manager Vendor Risk Management

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

Apply On Company Site

requirements.

- Stay abreast of regulatory environment regarding VRM.

Qualifications

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

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

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

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

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

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

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

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

4. *IARCP Authorized Certified Trainer (IARCP-ACT) Program* - This is an additional advantage on your resume, serving as a third-party endorsement to your knowledge and experience.

Certificates are important when being considered for a promotion or other career opportunities. You give the necessary assurance that you have the knowledge and skills to accept more responsibility.

To learn more, you may visit:
https://www.risk-compliance-association.com/IARCP_ACT.html

5. *Approved Training and Certification Centers (IARCP-ATCCs)* - In response to the increasing demand for CRCMP training, the International Association of Risk and Compliance Professionals is developing a world-wide network of Approved Training and Certification Centers (IARCP-ATCCs).

This will give the opportunity to risk and compliance managers, officers, and consultants to have access to instructor led training at convenient locations that meet international standards.

ATCCs use IARCP approved course materials and have access to IARCP Authorized Certified Trainers (IARCP-ACTs).

To learn more:
https://www.risk-compliance-association.com/Approved_Centers.html