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, September 27, 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,

I have just read the *Joint Committee Report on Risks and Vulnerabilities in the EU Financial System – September 2021,* from the European Supervisory Authorities. It is interesting to feel how the insurance sector worries about the risks in the banking sector.

We read: "Vulnerabilities in the banking sector could spill over to insurers and Institutions for Occupational Retirement Provision (IORPs), as they are interconnected with the banking sector through investments in assets issued by banks. At the end of 2020 on average approximately 13.7% (EUR 1,179 tn) of insurers' total investment is concentrated towards banks.

Over the course of last year insurers have reduced their exposure by approximately two percentage points. It is smaller for the IORPs sector compared to the insurance sector, but its exposure towards the banking sector is also material; this holds especially for some specific countries.

At the end of 2020, on average ca. 12% (EUR 140 bn) of IORPs total investment is concentrated towards banks."

We also read: "The European corporate sector has been significantly hit by the pandemic, but the extraordinary monetary and fiscal stimulus has helped mitigate its impact. PGS loans have facilitated the flow of lending and have been supportive in particular for the SME sector. PGS loans of a total volume of EUR 381bn in Q1 2021 nevertheless indirectly increase sovereign exposure and may contribute to an increase of the nexus between banks and the sovereign they are domiciled in.

Exposure to PGS loans is mostly concentrated to a few Member States only. In light of increasing levels of public debt in the pandemic, sovereign debt sustainability can have a direct impact on banks' balance sheets. Total direct exposure of EU banks towards general governments was at over EUR 3.2 trillion in Q4 2020. 51% of total direct exposure was towards the home country (50% in Q2 2020).

Similarly, in the insurance and IORP sector the risk that certain countries are more affected by the pandemic amplifies the concentration risk, both of which also have significant home bias in their investments. Looking through the bond portfolio, holdings of insurers and IORPs' bonds continue to show significant home bias, whereas home bias for corporate bonds, representing 30% (EUR 2,677 bn.) of insurers' portfolio, is lower compared to government bonds (EUR 2,748 bn. of total investments). Furthermore, one third of the corporate bonds (EUR 824 bn.) are issued by banks, adding additional vulnerabilities to insurers' portfolios."

I read the paper, and I have spent a couple of hours thinking about the *concentration risk*. Excessive concentrations of credit have been key factors in banking crises and failures. Non-credit concentrations include:

- elevated *interest rate risk* due to maturity concentrations;
- *liquidity risk* due to funding concentrations;
- *operational risks* associated with concentrations of certain lines of business, such as mortgage servicing.

Before the 2008 financial crisis, concentrations of commercial real estate (CRE) loans, energy loans, leveraged financing loans, collateralized debt obligations, counterparty credit, loans to emerging market countries, loan participations, and agricultural loans, played major roles in the failure or material weaknesses of a large number of banks.

Other credit concentrations, such as loans secured by first liens on residential real estate, have historically posed fewer problems. However,

during the recession beginning in 2008, the banking industry experienced significant losses in these exposures when the national housing market suffered broad declines in home values.

Read more at number 1 below. Welcome to our Top 10 list.

Best regards,

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

Number 7 (Page 25)

Forged in the Fires of 9/11: Partnerships, Challenges, and Lessons Learned 20 Years Later

Christopher Wray, Director, Federal Bureau of Investigation
International Association of Chiefs of Police Annual Conference

Number 8 (Page 34)

The BIS 90 Years exhibition and Open Week

Number 9 (Page 36)

Community Bank Access to Innovation through Partnerships

Federal Reserve Board

Number 10 (Page 38)

Robotrolling 2021/2

Number 1

Joint Committee Report on Risks and Vulnerabilities in the EU Financial System – September 2021

After over a year since the COVID-19 pandemic started, the financial sector has largely proved resilient in the face of its severe economic impact.

A range of fiscal, monetary and prudential response measures as well as the availability of capital buffers have been essential in dampening the impact of the crisis.

As the recovery begins, the appropriate phasing out of exceptional crisis measures plays a key role.

Despite the positive outlook, the expectations for economic recovery remain uncertain and uneven across member states. Vulnerabilities in the financial sector are increasing, not least because of side effects of the crisis measures, such as increasing debt levels and upward pressure on asset prices.

Also, expectations of inflation- and yield growth, as well as increased investor risk-taking and financial interconnectedness issues, might put additional pressure on the financial system.

Next to economic vulnerabilities, the financial sector is also increasingly exposed to cyber risk and informationand communication technology (ICT) related vulnerabilities.

Financial institutions have to rapidly adapt their technical infrastructure in response to the pandemic, and the crisis has acted as a catalyst for digital transformation more generally.

The reliance of the financial system on technology and the scope for cyber vulnerabilities have further increased.

The financial sector has been hit by cyber-attacks more often than other sectors, while across the digital economy cyber-criminals are developing new techniques to exploit vulnerabilities.

In light of the above-mentioned risks and uncertainties, the Joint Committee advises the ESAs, national competent authorities, financial institutions and market participants to take the following policy actions:

1. Financial institutions and supervisors should continue to be prepared for a possible deterioration of asset quality in the financial sector, notwithstanding the improved economic outlook.

In light of persisting risks and high uncertainties, supervisors should continue to closely monitor asset quality and provisioning in the banking sector, in particular of assets under support schemes. This includes identifying possible practices of under-provisioning.

Such monitoring is an important prerequisite when coordinating the unwinding of the various support measures.

2. As the economic environment gradually improves, the focus should in particular shift to allow a proper recognition of the consequences of the pandemic on banks' lending books, and that banks adequately manage the transition towards the recovery phase.

Banks may need to withstand possibly increasing credit risk losses, as a consequence of expiring payment moratoria and other public support measures, while maintaining adequate lending volumes.

Banks and borrowers experiencing financial difficulties should proactively work together to find appropriate solutions for their specific circumstances.

That should include not only financial restructuring, but also a timely recognition of credit losses. Other financial institutions, including investment funds, should monitor their investments in corporate bonds and into private lending.

3. Disorderly increases in yields and sudden reversals of risk premia should be closely monitored in terms of their impacts for financial institutions as well as for investors.

On the investor side, rising valuations across asset classes, massive price swings in crypto assets, and event-driven risks (such as GameStop, Archegos, Greensill) observed in 1Q21 amid elevated trading volumes raise questions about increased risk-taking behaviour and possible market exuberance.

Rising yields could result in higher funding costs for banks and increase default risks for corporates via higher borrowing costs.

Supervisors, policy makers and financial institutions should also continue to develop further actions to accommodate a "low-for-long" real

interest rate environment and risks its entails against the background of rising in inflation. This includes addressing overcapacities in the financial sector.

4. Policymakers, regulators, financial institutions and supervisors can start reflecting on lessons learnt from the COVID-19 crisis. While the EU economy is still subject to high risks, some lessons learnt have, for example, already been reflected in EIOPA's advice on the Solvency II review.

EIOPA recommends in its opinion that supervisors should have additional powers, including a macroprudential toolkit to tackle systemic risk, such as restrictions on distributions of dividends to preserve insurers' financial position in periods of extremely adverse developments.

In the banking sector, the crisis has underlined the need to advance the Banking Union, and to achieve its potential additional benefits of cross-border financial flows, private risk sharing, and exploiting economies of scale in a larger market.

The ongoing crisis also highlighted the critical importance of coordinated approaches among national competent authorities.

5. Financial institutions and supervisors should continue to carefully manage their ICT and cyber risks. They should ensure that appropriate technologies and adequate control frameworks are in place to address threats to information security and business continuity, including risks stemming from increasingly sophisticated cyber-attacks.

It will be important for EU financial institutions to achieve a high common level of digital operational resilience, and to swiftly put in place an EU-wide common framework for digital operational resilience.

An important aspect of digital operational resilience is proper management of risks around ICT outsourcing, including chain outsourcing. Additionally, there is increasingly a need for financial institutions to carry out resilience testing in proportion to the risks faced and in a consistent manner.

To read more:
https://www.eiopa.europa.eu/sites/default/files/joint-committee/jc-2021-45-joint-committee-autumn-2021-report-on-risks-and-vulnerabilities.pdf?fbclid=IwAR1kJP7I_WF41wzeot_GQAb1P2NbcLB1AnucPdb2eNeuV4167HJVzRBlRZk

JOINT COMMITTEE REPORT ON

RISKS AND VULNERABILITIES IN THE EU FINANCIAL SYSTEM

SEPTEMBER 2021

Number 2

ESAs highlight risks in phasing out of crisis measures and call on financial institutions to adapt to increasing cyber risks

The three European Supervisory Authorities (EBA, EIOPA and ESMA - ESAs) issued their second joint risk assessment report for 2021. The report highlights the increasing vulnerabilities across the financial sector, the rise seen in terms of cyber risk and the materialisation of event-driven risks.

As the recovery begins, the appropriate phasing out of exceptional crisis measures plays a key role. Despite the positive outlook, the expectations for economic recovery remain uncertain and uneven across member states.

Vulnerabilities in the financial sector are increasing, not least because of side effects of the crisis measures, such as increasing debt levels and upward pressure on asset prices.

Expectations of inflation- and yield growth, as well as increased investor risk-taking and financial interconnectedness issues, might put additional pressure on the financial system.

The financial sector is also increasingly exposed to cyber risk. The financial sector has been hit by cyber-attacks more often than other sectors, while across the digital economy, cyber-criminals are developing new techniques to exploit vulnerabilities.

Financial institutions will have to rapidly adapt their technical infrastructure in response to the pandemic, and the crisis has acted as a catalyst for digital transformation more generally.

Finally, the materialisation of event-driven risks (such as GameStop, Archegos, Greensill), as well as rising prices and volumes traded on crypto-assets, raise questions about increased risk-taking behaviour and possible market exuberance.

Concerns about the sustainability of current market valuations remain, and current trends need to show resilience over an extended period of time for a more positive risk assessment.

In light of the above-mentioned risks and uncertainties, the ESAs advise national competent authorities, financial institutions and market participants to take the following policy actions:

- financial institutions and supervisors should continue to be prepared for a possible deterioration of asset quality in the financial sector, notwithstanding the improved economic outlook;

- as the economic environment gradually improves, the focus should shift to allow a proper assessment of the consequences of the pandemic on banks' lending books, and banks should adequately manage the transition towards the recovery phase;

- disorderly increases in yields and sudden reversals of risk premia should be closely monitored in terms of their impacts for financial institutions as well as for investors;

- financial institutions and supervisors should continue to carefully manage their ICT and cyber risks.

The ESAs also consider that policymakers, regulators, financial institutions and supervisors can start reflecting on lessons learnt from the COVID-19 crisis.

To read more:
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2021/1019147/JC%202021%2045%20-%20Joint%20Committee%20Autumn%202021%20Report%20on%20Risks%20and%20Vulnerabilities.pdf

Number 3

ESMA Report on Trends, Risks and Vulnerabilities

esma European Securities and Markets Authority

Risk summary

EU financial markets continued their recovery during the first half of 2021 with valuations at or above pre-COVID-19 levels, as the global economic outlook improved, with COVID-19 vaccine roll-outs and amid sustained public policy support.

Fixed income valuations, notably for HY corporate bonds are now far above their pre-COVID-19 levels in a context of increasing corporate and public debt.

Increased risktaking behaviour has led to volatility in equity (e.g. GameStop related market movements) and crypto asset markets, as well as to the materialisation of event-driven risks such as in the case of Archegos or Greensill.

Going forward, we expect to continue to see a prolonged period of risk to institutional and retail investors of further – possibly significant – market corrections and see very high risks across the whole of the ESMA remit.

Current market trends will need to show their resilience over an extended period of time for a more positive risk assessment to be made.

The extent to which these risks will materialise will critically depend on market expectations on monetary and fiscal policy support, as well as on the pace of the economic recovery and on inflation expectations.

The report:
https://www.esma.europa.eu/sites/default/files/library/esma50-165-1842_trv2-2021.pdf

Number 4

The "SecureSME Tool"

The European Union Agency for Cybersecurity (ENISA) announces the creation of the "SecureSME Tool". A practical and user-friendly tool facilitating SMEs to navigate to ENISA's tips, guidelines and recommendation.

According to the European Commission's data, small and medium-sized enterprises (SMEs) constitute 99% of all businesses in the EU and employ around 100 million people.

In order to overcome the challenges imposed by the COVID-19 pandemic many SMEs applied new business continuity measures and turned to new technologies such as adopting to cloud services, upgrading their internet services, improving their websites, and enabling staff to work remotely.

Although SMEs have turned to new technologies, they often fail to raise the level of their security, mainly due to the lack of funding and cybersecurity guidelines.

The European Union Agency for Cybersecurity is providing continuous support to SMEs.

In doing so the "SecureSME" Tool has been created as a means to raise awareness and help SMEs become digitally secure.

The "SecureSME" tool is a one-stop shop for European SMEs, which provides related cybersecurity recommendations, guidelines and tips in a simplistic and user friendly manner.

The goal of the tool is to support those businesses in securing their ICT services and infrastructure from cyberattacks and ensure business continuity.

The tool will be presented and become directly accessible to the public on the 8th September 2021, within the framework of the International Cybersecurity Forum (FIC 2021) in Lille, France.

ENISA is an active participant to the fair dedicated to public and private cybersecurity operators, by running an awareness campaign dedicated to SMEs.

What is the "SecureSME" Tool?

Cybersecurity doesn't necessarily have to be costly for SMEs to implement and maintain. There are several measures that can be implemented, without having to invest a large amount.

ENISA's ''SecureSME Tool" is a dedicated platform designed to support small and medium size businesses in their efforts to become digitally secure. This is achieved through the provision of practical and concise cyber tips and guidelines on how to secure ICT infrastructure.

The "SecureSME" tool presents the following main sections of particular interest to SMEs:

- Cyber tips that include instructions on how to:

Protect Employees
Enhance Processes
Strengthen technical measures
Overcome Covid19 issues

- Videos

- Guidelines in relation to SME cybersecurity published by ENISA and Member States' National Authorities

- EU H2020 related projects

Background

"SecureSME" tool comes as the next step following the publication of the "Cybersecurity for SMEs" report by ENISA last June. The report provides SMEs with advice on how to successfully cope with cybersecurity challenges, particularly those resulting from the COVID-19 pandemic.

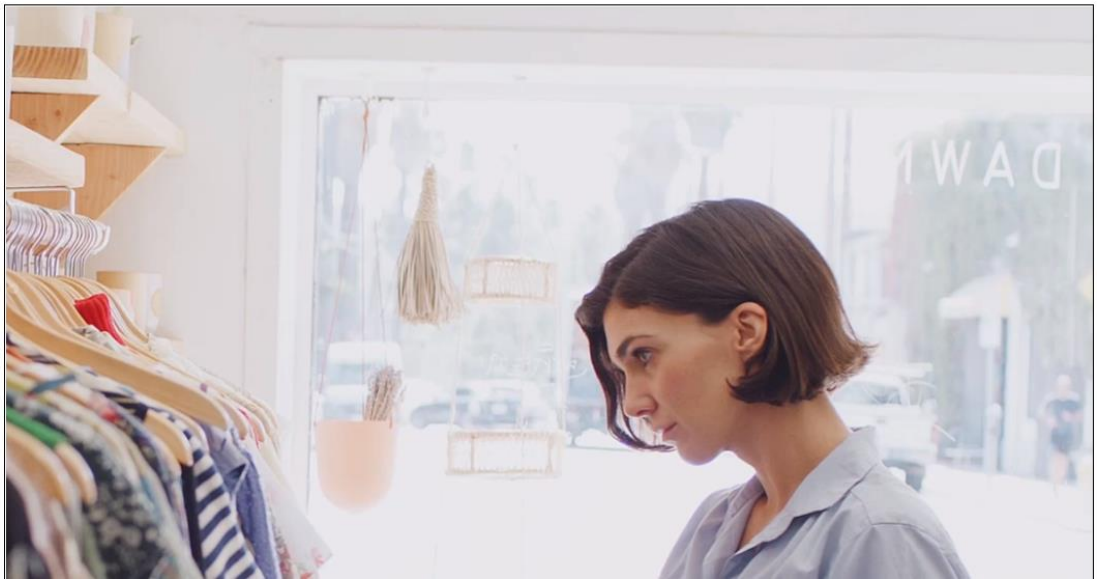
In addition to the report, ENISA also published a short cybersecurity guide in the form of a leaflet: "12 steps to securing your business", which provides SMEs with practical high-level actions to better secure their systems and hence their businesses.

To read more:
https://www.enisa.europa.eu/news/enisa-news/new-tool-is-another-step-towards-securing-the-digital-future-of-smes

https://www.enisa.europa.eu/securesme#/

Cybersecurity for SMEs - 12 steps to securing your business

Small and Medium-sized enterprises are facing major cybersecurity challenges. In a time of increased remote work and growing cyber threats, low security budget and lack of cyber-skills can seriously impact their competitiveness.



Discover all Cyber Tips

Protect Employees

Enhance processes

Strengthen technical measures

Overcome COVID19 issues

Number 5

Central bank digital currency: the future starts today

Benoît Cœuré, Head of the BIS Innovation Hub, at The Eurofi Financial Forum, Ljubljana

Distinguished guests, ladies and gentlemen.

Thank you for inviting me to speak here today. We all experienced how the pandemic accelerated the shift to virtual events, but I am pleased that today we are gathering in person.

Yet the world is not returning to the old normal. Payments are a case in point. The pandemic has accelerated a longer-running move to digital.

Mobile and contactless payments are already part of our daily lives; QR codes and "buy now, pay later" options are gaining popularity; gloves, badges and Olympic uniforms with payment functions are being prepared for the Beijing Winter Olympics; and the tech-savvy generation will soon dream about money and payments for the metaverse.

Alongside these developments, the world's central banks are stepping up efforts to prepare the ground for digital cash – central bank digital currency (CBDC). They have a job to do – delivering price stability and financial stability – and they must retain their ability to do it.

Let me explain.

Central bank money has unique advantages – safety, finality, liquidity and integrity. As our economies go digital, they must continue to benefit from these advantages.

Money is at the heart of the system and it has to continue to be issued and controlled by trusted and accountable institutions which have public policy – not profit – objectives.

Central bank money will have to evolve to be fit for the digital future.

So what are the priorities now? Know where you are going – as Dag Hammarskjöld once said2, "only he who keeps his eye fixed on the far horizon will find the right road". And get going.

Let me elaborate.

Why do we need to know where are we going? Because today, the financial system is shifting under our feet.

Big techs are expanding their footprint in retail payments. Stablecoins are knocking on the door, seeking regulatory approval. Decentralised finance (DeFi) platforms are challenging traditional financial intermediation. They all come with different regulatory questions, which need fast and consistent answers.

Banks are worried about the implications of CBDCs for customer deposits. Central banks are mindful of these concerns and are working on answers. They see banks as part of future CBDC systems. But make no mistake: global stablecoins, DeFi platforms and big tech firms will challenge banks' models regardless.

Stablecoins may develop as closed ecosystems or "walled gardens", creating fragmentation. With DeFi protocols, any concerns about the assets underlying stablecoins could see contagion spread through a system. And the growing footprint of big techs in finance raises market power and privacy issues, and challenges current regulatory approaches.

Will the new players complement or crowd out commercial banks? Should central banks open accounts to these new players, and under which regulatory conditions? Which kind of financial intermediation do we need to fund investment and the green transformation? How should public and private money coexist in new ecosystems – for example, should central bank money be used in DeFi rather than private stablecoins?

We urgently need to ask ourselves these kinds of questions about the future. This is the far horizon for the financial system but we are approaching it ever faster. Central banks need to know where they want to go as they embark on their CBDC journey.

CBDC will be part of the answer. A well-designed CBDC will be a safe and neutral means of payment and settlement asset, serving as a common interoperable platform around which the new payment ecosystem can organise. It will enable an open finance architecture that is integrated while welcoming competition and innovation. And it will preserve democratic control of the currency.

This brings me to my second message: the time has passed for central banks to get going. We should roll up our sleeves and accelerate our work on the nitty-gritty of CBDC design. CBDCs will take years to be rolled out, while stablecoins and cryptoassets are already here. This makes it even more urgent to start.

In the design thinking methodologies we use in the BIS Innovation Hub, the ideal product stands in a sweet spot at the intersection of desirability, viability and feasibility. When applied to CBDCs, these translate into three dimensions: consumer use cases, public policy objectives and technology.

We have to ask ourselves why consumers would want a CBDC and what would they want it to do? The recent European Central Bank (ECB) public consultation showed that they value privacy, security and broad usability.

In order to meet consumers' expectations, CBDCs need to be made to work most conveniently. Payment data must be protected. Digital functions that are not available with cash can be developed, such as programmability or viable micro-payments.

Then CBDCs should meet public policy objectives. Central banks exist to safeguard monetary and financial stability for the public good. CBDCs are a tool to pursue this through enhancing safety and neutrality in digital payments, financial inclusion and access, innovation and openness. Important questions remain. How can CBDC systems interoperate, and should offshore use be discouraged?

Technology opens up design choices. System design will be complex. It involves a hands-on operational and oversight role for central banks and public-private partnerships to develop the core features of the CBDC instrument and its underlying system. These features are: ease of use, low cost, convertibility, instant settlement, continuous availability and a high degree of security, resilience, flexibility and safety.

Complex trade-offs will be addressed by central banks including how to balance scale, speed and open access with security; and how to balance offline functionality with complexity and security.

Across the world, central banks are coming together to focus on their common mission. Charged with stability, they will not rush. They want to move fast, but not to break things.

Consultations with payment systems and providers, banks, the public and a broad range of stakeholders have begun in some countries. To build a CBDC for the public, a central bank needs to understand what they need, and work

closely with other authorities. The BIS Innovation Hub is helping central banks. We already have six CBDC-related proofs of concept and prototypes being developed in our centres, and more to come.

The European Union is uniquely placed to face the future. You can build on a state-of-the-art fast payment system, on the strong protections provided by the General Data Protection Regulation and on the open philosophy of the Second Payment Services Directive. The ECB's report on a digital euro sets the stage.

A CBDC's goal is ultimately to preserve the best elements of our current systems while still allowing a safe space for tomorrow's innovation. To do so, central banks have to act while the current system is still in place – and to act now.

I thank you for your attention.

Number 6

Basel III implementation in the European Union

Introductory remarks by Pablo Hernández de Cos, Chair of the Basel Committee on Banking Supervision and Governor of the Bank of Spain, Eurofi panel on Basel III implementation in the EU, Ljubljana

Good morning and welcome to this panel on implementing Basel III in the EU.

When I was asked to chair this panel (in my capacity as Chair of the Basel Committee), I must confess that I had somewhat mixed feelings.

On the one hand, I was pleased to see that Eurofi was organising this one-hour panel to discuss what is a crucially important topic. As you know, following the Great Financial Crisis (GFC), the Basel Committee undertook a range of reforms to address material regulatory fault lines in the banking system.

The benefits of the initial set of reforms – which were aimed at addressing the unsustainable levels of leverage in the banking system, insufficient high-quality capital, excessive maturity transformation and lack of a macroprudential overlay – were clear to all of us during this pandemic.

The global banking system has remained broadly resilient to date, and, unlike during the GFC, banks have not exacerbated the economic crisis by sharply cutting back lending. The initial Basel III reforms, alongside an unprecedented range of public support measures, are the main explanations for this outcome.

In many ways, Covid-19 has provided clear and tangible evidence of the benefits to society in having a well-capitalised banking system. We saw that jurisdictions with banks that had the largest capital buffers experienced a less severe impact on their expected GDP growth and better-capitalised banks increased their lending more during the pandemic relative to their peers.

Yet the job of safeguarding global financial stability is far from finished. The outstanding Basel III reforms, which were finalised in 2017, are aimed at addressing significant fault lines in the global banking system.

Addressing these fault lines remains as important today as it was pre-pandemic. Indeed, the primary objective of these reforms is to restore credibility in the risk-weighted capital framework. This is to be achieved by reducing excessive variability in banks' modelled capital requirements and developing robust risk-sensitive standardised approaches which would also serve as the basis of the output floor.

Recall how at the peak of the GFC investors lost faith in banks' published ratios and placed more weight on other indicators of bank solvency. Whether due to a lack of robustness in banks' models or an excessive degree of discretion in determining key regulatory inputs, the shortcomings in the risk-weighted asset (RWA) framework underlined the need for a complete overhaul.

Let me just give one example to underline how these fault lines continue to remain a major concern today. In 2013, the Committee's first report on the variability of banks' risk-weighted assets highlighted a worrying degree of variation.

When banks were asked to model their credit risk capital requirements for the same hypothetical portfolio, the reported capital ratios varied by 400 basis points.

Fast-forward to 2021 – eight years later – and despite repeated claims by some stakeholders that banks have already "fixed" this problem, the latest report by the European Banking Authority on banks' modelled capital requirements points to a "significant" level of capital dispersion "that needs to be monitored".

Importantly, these Basel III reforms are not an exercise to increase overall capital requirements at a global level. But equally, to successfully meet our primary objective, "outlier" banks, such as those with particularly aggressive modelling techniques, will rightly face higher requirements.

Given the "exogenous" nature of the Covid-19 shock, these vulnerabilities were not tested during this pandemic.

However, it is clear that, if left unaddressed, they will expose material shortcomings in the banking system in future financial crises. So I am pleased that we will have the opportunity this morning to discuss the implementation of these reforms in the EU.

On the other hand, I remain concerned about the potential to focus the discussion on whether or how to implement Basel III in the EU in the current juncture! These reforms were finalised in 2017, with a globally

agreed (revised) implementation date of 1 January 2023. G20 Leaders have repeatedly called for their full, timely and consistent implementation. Now is therefore the time for action.

It is increasingly clear that the outstanding Basel III reforms will complement the previous ones in having a positive net impact on the economy.

For example, a recent analysis by the ECB suggests that the GDP costs of implementing these reforms in Europe are modest and temporary, whereas their benefits will help to permanently strengthen the resilience of the economy to adverse shocks.

It also finds that potential deviations from the globally agreed Basel III reforms – for example, with regard to the output floor – would significantly dilute the benefits to the real economy.

Importantly, the reforms also benefited from an extensive consultation process with a wide range of stakeholders. Indeed, a recent academic study described the Committee's consultation approach as "one of the most procedurally sophisticated" processes among policymaking bodies.

The Committee published no fewer than 10 consultation papers as part of these reforms, with an accompanying consultation period that spanned the equivalent of almost three years!

So the finalised standards agreed at the global level are already a compromise by their very nature, and reflect the different views of Committee members and external stakeholders. Over 35 key adjustments were made to the reforms during this period, with the majority of these reflecting the views of different European stakeholders.

Financial stability is a global public good. It knows no geographic boundaries – the adage that "no one is safe until everyone is safe" applies as much to the pandemic as it does to safeguarding global financial stability.

This is why the Committee designed and calibrated Basel III at a global level, and incorporated enough flexibility through national discretions within the framework.

Approaching these reforms from a different perspective – for example by giving undue attention to the impact on individual banks, jurisdictions or regions – risks missing the forest for the trees.

To be clear: the domestic and democratic transposition of global standards is a very important process and one that should be fully respected. But the focus should now primarily be on the "action" side of things, which means demonstrating how the EU's commitment to multilateralism and to globally agreed decisions endorsed by the Group of Governors and Heads of Supervision, and to which G20 Leaders have repeatedly committed to implementing in a full, timely and consistent manner.

So I hope that our panel discussion today and the active participation of the audience will provide a constructive discussion on these important issues, building on the broad landscape that I have just set out.

Number 7

Forged in the Fires of 9/11: Partnerships, Challenges, and Lessons Learned 20 Years Later

Christopher Wray, Director, Federal Bureau of Investigation
International Association of Chiefs of Police Annual Conference

Thank you for the introduction, Cynthia, and thank you for inviting me to speak to IACP once again. Obviously, our hearts go out to everyone affected by Hurricane Ida—especially our colleagues in law enforcement and emergency response. And I'm grateful to everyone at IACP for pivoting so quickly and making it possible for us to meet virtually.

In our line of work, confronting and adapting to the unexpected is part of the job. Never was that more true than 20 years ago today—September 11, 2001 was one of the darkest days our nation has ever faced.

Just this morning I was in New York for the memorial ceremony, where family and friends read aloud the names of the nearly 3,000 innocent lives lost that day. Among them were more than 400 first responders—including more than 70 law enforcement officers.

The FBI lost two of our own that day: Special Agent Lenny Hatton and former Special Agent John O'Neill. That day, Lenny and John and hundreds more heroic men and women did what first responders always do: They put others before themselves and did whatever it took to rescue people and save lives.

On this solemn anniversary, we resolve once more to "never forget": to never forget the lives we lost on 9/11, to never forget the colleagues we've lost to 9/11-related illnesses since then, and to never forget the incredible bravery and sacrifices of our police, firefighters, and emergency personnel.

But there's one more thing I know you'll agree we should never forget—the spirit of unity and shared purpose that brought our nation together on September 12 and in the weeks and months that followed.

We in law enforcement and intelligence also felt that incredible spirit of solidarity in those days after 9/11. We'd always known that partnerships were important in our profession—but after that day, we realized they were something we couldn't function without. To prevent more 9/11s, we knew we had to build even stronger partnerships, work together even more closely, and share information even more seamlessly.

We've spent the last 20 years doing just that, together. And the changes we've made and the hard work we've done over those two decades have helped keep our country safe. That's something we should all be proud of.

Still, we can never rest on our laurels, because the threats keep shifting, and the challenges keep coming. So this afternoon, I want to talk to you about some of those challenges—and why the deeper partnerships we forged in the fires of 9/11 are so critical to confronting the threats we're up against today.

Lessons Learned

Twenty years ago, 9/11 forced those of us in law enforcement and intelligence to take a hard look at ourselves. At the FBI, we asked ourselves—what did we miss? What could we have done better to stop the attack before it happened?

Because of that terrible day, the Bureau transformed itself in ways that have made us stronger and better—and our country safer. And we couldn't have done it without your help.

We became an intelligence-driven, national security and law enforcement organization—one that collects, uses, and shares intelligence in everything we do. We developed new capabilities to combat the terrorist threat. And we changed our focus from investigating terrorist plots and attacks after the fact, to stopping them before they occur.

We built more integral partnerships with our law enforcement and intelligence community colleagues—starting by expanding and strengthening our task forces. They've grown, in fact, thrived in collaboration with hundreds of your departments nationwide, as we continue the critical work of protecting our country in a post-9/11 world. And in field office after field office, I see and hear how seamlessly our task force officers and agents work together.

Time and time again, when we've disrupted would-be terrorists before they strike; those cases have been driven by your frontline observations and your eagerness to share that reporting. That's why our partnerships remain

paramount in the fight against terrorism. And that includes our partnerships with community leaders, which we've also worked hard to improve since 9/11.

September 11 also taught us painful yet crucial lessons about the need to avoid complacency, and the need to keep innovating—because, as 19 hijackers armed with nothing more than box cutters showed us, the bad guys never stop innovating.

All these years later, the FBI still feels the ripple effects of the evolution in how we tackle our work. And not just in counterterrorism. We've applied the lessons we learned from 9/11 to every FBI program and every investigation, in every community we serve.

Current Terrorism Threat Picture

Of course, even as we all evolved in how we combat terrorism, the terrorist threat itself evolved as well.

Two decades after 9/11, we still face threats from al Qaeda and other foreign terrorist groups that want to carry out large-scale attacks here in the United States and around the world.

Some of those groups, like ISIS, use social media both to spread propaganda and to recruit and inspire followers to attack wherever they can, in whatever way they can. We also continue to track state-associated groups, like Iran's Islamic Revolutionary Guard Corps, that pose threats both at home and abroad.

But we also know that today's terror threat is different from what it was 20 years ago.

Today, the greatest terrorist threat we face in the U.S. is from lone actors. These include not only homegrown violent extremists, who take inspiration from foreign terror groups and ideologies, but also domestic violent extremists—especially racially or ethnically motivated violent extremists, and anti-government or anti-authority violent extremists.

Far too often, we're seeing people resort to violence to advance their ideological, political, or social goals. That's why, throughout the last year, the FBI has significantly surged resources to our increasing number of domestic terrorism investigations.

Bottom line: 20 years after 9/11, preventing terrorist attacks remains the FBI's top priority—now and for the foreseeable future.

Violent Crime Surge

But even as we counter the terrorism threat, we're staying laser focused on violent crime in our cities and communities. Mass shootings, gun violence, homicides, and aggravated assaults are all occurring at an appalling rate across the country, along with an uptick in reported hate crimes.

Today's violent crime situation is hellishly challenging—and for the Americans caught in the crosshairs of this surge in violent crime, it's just plain hell.

Like in Louisville, where homicides went up 92% in 2020—and are on pace this year to eclipse that, with more than 20 of those murder victims innocent children. Or in Dallas, or Milwaukee, where aggravated assaults are up—with Milwaukee, in particular, on track to surpass their 2020 rates for homicides, shootings, and carjackings, all by the end of this year.

Meanwhile, gangs in places like Memphis, Louisville, Chicago, and Oklahoma City are establishing narcotics pipelines to traffic heroin and other drugs throughout the Midwest and South. And in Phoenix, local gangs are working with transnational organized crime groups, helping them traffic people, drugs, and firearms throughout the Southwest.

Everyone listening to me knows all too well that the violent crime surge in our country is real and growing. It's taking the lives of too many innocent people, tearing apart too many communities, and denying too many Americans their basic right to feel safe in their own homes and neighborhoods.

Now I realize I'm preaching to the choir—because we all know that at all levels of government, our most fundamental duty is to safeguard people's right to live without fear of violence.

To meet this duty, we in the FBI know we've got to stand in lockstep with our law enforcement partners, now more than ever. And I can assure you we're using all of our tools and working strategically with our partners to face the violent crime surge head-on.

FBI Resources to Tackle Violent Crime

Across the country, we're determined to tackle violent crime together through our FBI Violent Crime, Safe Streets, and Safe Trails task forces. Just last year, our Safe Streets Task Forces made more than 6,000 arrests, seized more than 4,000 guns, and dismantled 80 violent gangs across the country.

To build on those task force efforts, in the coming months, the FBI will deploy new rapid response teams to some of the places hardest hit by the increased violence.

We'll be sending agents and intelligence analysts, surging resources and leveraging the intelligence we gather from violent crime investigations to help crack down on violent gangs and disrupt multi-state criminal enterprises.

As we confront the massive rise in violent crime, at the FBI it's all hands on deck—with every part of the Bureau, not just our violent crime task forces, sharing intelligence and resources to help our state, local, and tribal partners.

The FBI Lab is providing forensic analysis and testimony, shooting incident reconstruction, and support for searches of the 20 million DNA profiles in our National DNA Database.

The FBI-led National Gang Intelligence Center is supporting investigations with timely information on gang migration and criminal activity.

Our CJIS Division is working 24/7 to provide crucial data through systems like NCIC, NICS, and Next Generation Identification.

Our Critical Incident Response Group is deploying command post operations, tactical response, crisis negotiation, and behavioral analysis.

And our Victim Services Division is standing by to provide operational and victim support in crisis and mass-casualty events.

In all these ways and scores more, you can count on the entire FBI to stand shoulder-to-shoulder with you in the fight against violent crime.

The recent violent crime surge is a big challenge for all of us, and the way we'll meet it is with the same intelligence-driven, partnership-grounded approach that we've used successfully against the terrorist threat since 9/11.

Threats to Law Enforcement

Unfortunately, it's not just dangerous out there for the people we protect and serve; it's also dangerous for our officers, agents, and deputies. I want to sound the alarm again about another kind of emergency—one that threatens the very people Americans rely on to keep them safe.

Over the past year, we've seen a surge of violence against the law enforcement community. In just the first eight months of this year, 50 law enforcement officers have been feloniously killed on the job in our country—that's more than in all of 2020. Let me say that again, there have been 50 officers murdered this year while doing their job to keep their communities safe.

I know some of you are all too familiar with the pain of losing your own in the line of duty. We are, too. Earlier this year two of our special agents, Laura Schwartzenberger and Dan Alfin, were shot and killed while serving a search warrant in Florida. And in July, one of our longtime task force officers, Detective Greg Ferency of the Terre Haute, Indiana, Police Department, was shot and killed in an ambush right outside one of our offices. Three of our own, murdered in just a few months.

As I never tire of telling people, it takes an incredibly special person to put his or her life on the line for a total stranger, day after day. When I started this job a little over four years ago, I made a point to know when any officer is murdered in the line of duty, so I can call the chief or sheriff of that department to offer the FBI's condolences and support.

Since August 2017, I've made more than 200 of those calls.

Enough is enough. As a country, we cannot blind ourselves to the sacrifices that law enforcement officers make every day. All of us—their law enforcement colleagues and the citizens they died protecting—owe these dedicated public servants a debt of gratitude.

Mental Health

Given all we're up against, it's no wonder that many of your officers feel beleaguered, underappreciated, and under siege. Which is why I want to turn to an issue that's sometimes hard to discuss, but vital to address—and that's the mental health and well-being of our people.

Our officers and agents offer a lot of the best humanity has to offer. Courage. Selflessness. Honor. But to do their jobs, they have to confront the worst that humanity has to offer.

That kind of ongoing stress and pressure is a lot of weight to carry, day after day. It's likely one of the reasons suicides have become an epidemic in law enforcement—and hardly any agency is immune. Last year, there were 174 officer suicides in our country.

We need to figure out exactly what's going on. That's why the FBI's Uniform Crime Reporting program is establishing a new data collection effort to better understand and prevent suicides among current and former law enforcement officers. Agencies can submit information about their officers who have attempted or died by suicide—and getting that information from all of you and the rest of our partners is essential.

Because when it launches next year, UCR's collection will include data on the circumstance and events before each suicide and attempt. The results—that intelligence—will be crucial to understanding the problem and finding solutions before it is too late.

But even more importantly, just as we do in every other battle, we need to draw on our partnerships. In this case, that means being the best possible partner to colleagues who are hurting and getting rid of the stigma that stops folks from seeking help.

These aren't 9-to-5 jobs with 9-to-5 pressures. So we need to tell our people it's okay to not be okay. It's okay to admit that—because that's not a sign of weakness, it's a sign of real strength. And we shouldn't wait. Taking care of ourselves and one another should be an all-the-time thing, not just something we think about when things become unbearable.

We want all our people around for the long haul—the country needs them around for the long haul—so let's make sure we're getting them the help they need, and let them know we're going to stand beside them, every step of the way.

Our Work: The Right Thing in the Right Way

Since becoming FBI Director, I've tried to drive home the importance of always doing the right thing, in the right way. The 20th anniversary of 9/11 is a fitting reminder of why that's so important.

9/11 showed us just how much is on the line in our work, how we're always just one attack away from a tragedy will change people's lives forever. Millions of people we'll never know are counting on us to do our jobs well—to get it right.

After 9/11, appreciation for law enforcement and our fellow first responders was near-universal. Folks understood that our work was about doing the right thing, and they recognized the nobility of our mission. A rising generation saw that, and as a result, scores of young people chose to pursue public service, including in law enforcement.

Twenty years later, we have fewer and fewer people who either worked for us during 9/11 or joined our ranks because of 9/11. It sounds hard to believe, but we now have agents and analysts joining the FBI who were only in elementary school when the 9/11 attacks happened—and in a few years we'll be hiring folks who weren't even alive on that fateful day.

So we need to make a special effort to ensure that September 11 and its lessons don't become some historical footnote—especially in the current environment, when the negativity surrounding law enforcement has made recruiting tough for so many departments.

There's no question that law enforcement remains a noble profession. And I truly believe that—although sometimes it may not seem like it—folks still recognize and appreciate the sacrifices our people make.

As a new generation enters our ranks, it falls on those of us who lived through the post-9/11 transformation of our work to show them why it's so crucial to do things the right way. That takes a lot when your work is as hard and consequential as ours is—from precision and rigor, to uncompromising integrity, to following the facts wherever they lead, no matter who likes it. It also means setting aside concerns about who gets credit, and focusing on impact.

We've all seen firsthand how the shift away from turf battles and stove-piping, to sharing intelligence and strengthening our partnerships, gets results that keep people safer. And now the young men and women in our departments, who listen to and learn from us, don't know any other way than that post-9/11 shoulder-to-shoulder approach.

That's how it should be. That's how it needs to be. 9/11 should always remind us that we can't go back to the old ways. Because when we work in the right way, together—when we combine our unique capabilities and authorities, our strengths and assets—we're so much stronger than when we do the job alone.

Conclusion

I began today by recalling the solidarity and spirit of September 12, and the enduring resilience of this country and of our law enforcement family. There's perhaps no better symbol of that resilience than the Survivor Tree, which stands as part of the 9/11 Memorial in New York City.

A month after the terrorist attacks, recovery workers discovered a Callery pear tree buried in the rubble of the Twin Towers. It was badly damaged, its roots snapped, and its branches broken and burned. The tree was dug up

from the ruins and placed in the care of the New York City Department of Parks and Recreation. They replanted it in a park in the Bronx, where it wasn't expected to survive.

But over the years, that pear tree recovered. It was returned to the 9/11 Memorial back in 2010. Today, smooth limbs extend from the tree's gnarled stumps, clearly showing the line between the tree's past and present—before 9/11 and after. It stands at the memorial as a living reminder of our country's enduring spirit and resilience.

Like that tree, our law enforcement family has its own clear line in our history—before 9/11 and after. We learned hard lessons from that terrible day. And we've experienced our own rebirth—one that has helped us to better protect all the people who are counting on us.

Thank you all for your leadership, and your partnership with the FBI. And thanks for listening to me today.

Number 8

The BIS 90 Years exhibition and Open Week

The BIS 90 Years exhibition and Open Week will showcase the Bank's unique role in the global financial system, looking at its history since 1930 and with a particular focus on the BIS today and tomorrow.

The interactive, multimedia BIS 90 Years exhibition was developed and designed in collaboration with Basel design agency berger + Co.

The exhibition will be displayed over three levels of the iconic BIS Tower building in Basel, including the 18th floor with its bird's eye view over the city and the surrounding area.

BIS 90 Years will introduce visitors to the BIS's role and activities in an accessible way and cover some of the major issues facing central banks, such as the digital revolution in finance.

Interactive installations will bring to life the role money plays in our modern society. Visitors will also be able to map financial flows around the world in times of crisis and learn about the BIS's 63 member central banks.

The BIS is a forum for dialogue and international cooperation and a meeting place for central bankers and financial regulators, and hosts several standard setters for the international financial system.

It also promotes responsible innovation and knowledge-sharing, acts as a think tank for the central bank community and serves as a bank for central banks and international financial institutions.

BIS 90 Years will run from 26 October to 4 November, with a media preview on 22 October. Entry is free. Further details can be found on the dedicated website: www.bis90.org

BIS 90 Years was originally planned for 2020, at the time of the Bank's 90th anniversary, but was postponed due to the pandemic. Strict safety measures will apply, in full accordance with official Swiss Covid-19 guidelines and Swiss Museums Association recommendations.


Exhibition information
BIS 90 YEARS
Visitor information
DE / EN
OPEN
BIS
90
YEARS
26.10
—04.11
WEEK

Number 9

Community Bank Access to Innovation through Partnerships

Federal Reserve Board

Community banks in the United States are increasingly partnering with third-party financial technology companies (fintechs) to access innovation.

The Federal Reserve supports responsible innovation that provides community banks access to new technologies, while ensuring safety and soundness of the institutions and protection of consumers.

Under the right circumstances and with the appropriate guardrails, partnerships with fintechs can provide community banks with this access, enabling them to better serve their customers and deploy innovations that may be too costly to develop independently.

In a 2020 speech, Federal Reserve Board member Michelle W. Bowman stated that "the successful integration of financial technology into the community bank business model is proving to be enormously valuable to enable community banks to enhance the services they've already proven they can deliver effectively.

Access to technology and services to meet customer needs is critical to ensuring community banks remain vibrant."

This paper is intended to serve as a resource for community banks as they embark on responsible innovation. It provides an overview of the evolving landscape of community bank partnerships with fintechs, including the benefits and risks of different partnership types, and key considerations for engaging in such partnerships.

While these lessons may apply broadly to the community bank sector, each institution should evaluate how fintech partnerships fit into their own strategic objectives based on their research, risk profile, and third-party risk management practices.

The insights in this paper are based on engagements with a variety of outreach participants and do not reflect the view of the Federal Reserve

Board of Governors, the Federal Reserve Banks, or the staff of the Federal Reserve System.

This paper does not establish new or interpret existing guidance related to third-party risk.

The information in this paper was obtained through conversations held outside of the supervisory process for exploratory purposes and does not contain information that could be used to uniquely identify individual institutions or partnerships.

For further innovation work completed by the Federal Reserve Board of Governors, or to contact Federal Reserve staff about this paper, please visit the Federal Reserve Board's Innovation web page.

Figure 1. Strategic needs a community bank might consider when partnering with a fintech

Each partnership type between a community bank and a fintech targets specific needs and objectives of a community bank.

To read more:
https://www.federalreserve.gov/publications/files/community-bank-access-to-innovation-through-partnerships-202109.pdf

Number 10

Robotrolling 2021/2

In this edition of Robotrolling we track the most significant increase in inauthentic Russian-language social media activity we have observed since we began in 2017.

While the level of bot activity remains much lower than four years ago, the uptick is concerning.

The increased activity coincided with the spring and summer military exercise season, and the period running up to the Russian Federation's Zapad exercises, scheduled for September 2021.

While fake activity increased in the Russian-language space, we observed no increase in English-language activity, either from bots or from human-controlled accounts.

In this edition of Robotrolling, we introduce the *Global Database of Events Location and Tone (GDELT)*.

This database of news articles helps map how the conversation about NATO in Poland and the Baltics is covered by news media, and serves as a contrast to the environment observed on Twitter and VK.

This contrast reveals that in April 2021—as Russian troops mobilized along the Ukrainian border—inauthentic Russian accounts were also disproportionately active online.

We round off the issue with a discussion of how AI can help us better understand the global news environment in near-realtime, based on conversations with StratCom COE expert Gundars Bergmanis-Korāts and GDELT-founder Kalev Leetaru.

In this edition of Robotrolling, we continue to track manipulation on social media platforms about the NATO presence in Poland, Estonia, Latvia, and Lithuania.

Our analysis focuses on the activities of automated accounts (bots) and coordinated anonymous human accounts.

With this—our seventeenth—issue we are making a change to publishing the report biannually, with six-month reporting windows.

The period currently under consideration in this spring/summer issue is 1 February to 31 July 2021.

This window is compared and contrasted with the previous six months, 1 August 2020 to 31 January 2021.

In the Russian-language information space automated activity has increased markedly in the previous six months.

Currently, 36% of tweets come from automated accounts, constituting a 50% increase compared to the previous period.

English-language automated activity has also increased, but from a much lower comparative baseline.

Not only was bot messaging more widespread, but we also note a divergence in Russian- and English-language messaging volumes: the number of English messages (excluding retweets) about the NATO presence was unchanged at 11 200; Russian-language messages increased by 40% to 7 200.

On VK, the total messaging volume increased from 43 000 to 58 000 — a 35% increase.

Simultaneously, the percentage of automated Russian-language accounts increased on Twitter from 16% to 19% and on VK from 14% to 16%.

Automated activity on VK this quarter mirrored our findings for Twitter.

The proportion of bot activity increased along with message volume.

On VK, 56% of messages were posted in groups, an increase from 51% in the previous period.

The increased bot levels for spring and summer 2021 are a statistical outlier.

Since starting our observations in 2017 the overall trend has been for gradually declining levels of automated activity on Twitter, thanks to the company's efforts to clean up the platform.

The trend has stalled and may now even have reversed.

This change in trajectory coincides with the run-up to the Russian military's Zapad exercises to take place in September 2021.

As ever, social media companies should not rest on their laurels thinking the battle against bots has been won.

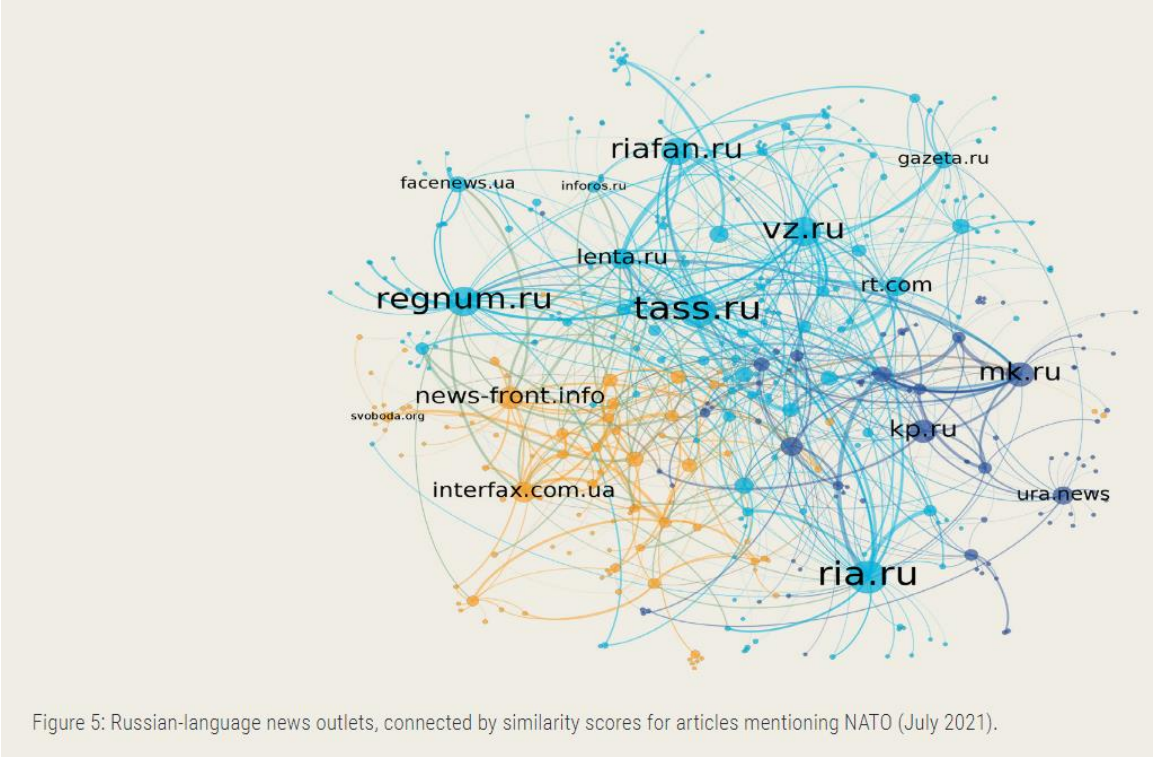


Figure 5: Russian-language news outlets, connected by similarity scores for articles mentioning NATO (July 2021).

To read more:
https://stratcomcoe.org/publications/robotrolling-20212/214

Disclaimer

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

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

This information:

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

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

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

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

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

- is in no way constitutive of an interpretative document;

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

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

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

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

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

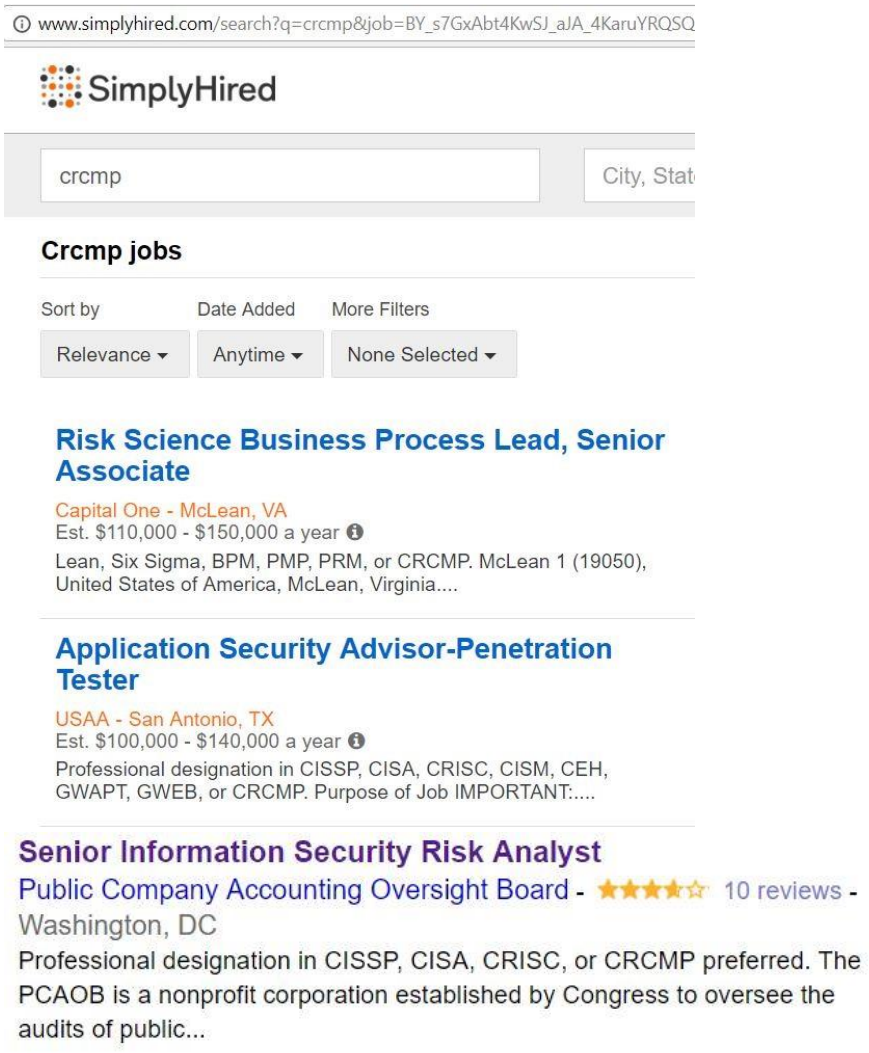
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

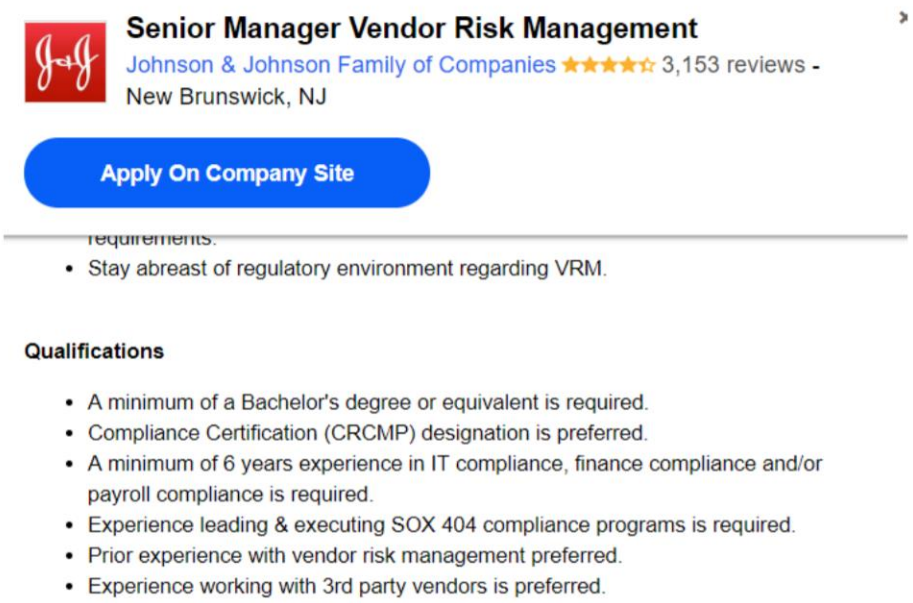
You can explore what we offer to our members:

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

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

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





Senior Manager Vendor Risk Management

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

Apply On Company Site

requirements.

- Stay abreast of regulatory environment regarding VRM.

Qualifications

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

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

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

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

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

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

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

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