Monday, June 22, 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,

I have just listened to an interesting podcast from Chris Woolard, Interim Chief Executive of the Financial Conduct Authority (FCA). FCA has rapidly reprioritised work in light of the coronavirus (Covid-19) pandemic.

One of the interesting areas covered is the *Business Interruption (BI) insurance,* that protects businesses from loss of profit or revenue, following an insured loss or damage to property and goods. It covers the gap in income from the time of the interruption to the time business returns to normal.

According to the FCA, the coronavirus pandemic has led to widespread disruption and business closures resulting in substantial financial loss. Many customers have made claims for these losses under their BI insurance policies.

There has been widespread concern about the *lack of clarity and certainty* for some customers making these claims, and the basis on which some firms are making decisions in relation to claims.

The issues surrounding BI policies are complex and have the potential to create ongoing uncertainty for both customers and firms. The variation in the types of cover provided and wordings used mean it can be difficult to determine whether customers have cover and can make a valid claim.

There are genuine doubts over the appropriate interpretation of the wording in some cases. This has led to uncertainty and disputes, with many customers who believe they have valid claims having these rejected by their insurer.

The FCA believes that the circumstances of the current coronavirus emergency, and its effect on businesses holding BI policies means this uncertainty needs to be resolved as quickly as possible.

Read more at number 7 below.

At number 5 below, there is another interesting presentation from Isabel Schnabel, Member of the Executive Board of the European Central Bank, with title: "The European Central Bank's policy in the COVID-19 crisis - a medium-term perspective".

We read that evidence is increasingly pointing towards a protracted impact of the crisis on both demand and supply conditions in the euro area and beyond.

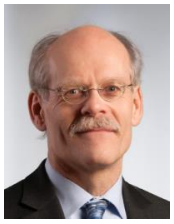
For central banks, this implies a shift in focus *from economic "firefighting"* – ensuring orderly market functioning and a sufficient provision of liquidity – to dealing with the implications of the crisis on *medium-term* inflation.

Isabel Schnabel explains why the *pandemic emergency purchase programme (PEPP)* remains the appropriate tool to address the current challenges of the crisis.

Welcome to the Top 10 list.

Best regards,

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



PRISM National Defense University Press
The premier professional military and academic publishing house

PCAOB
Public Company Accounting Oversight Board

Number 6 (Page 18)

Tips for secure user authentication

In an era of large-scale data breaches, The European Union Agency for Cybersecurity shares its recommendations for improving the security of passwords and authentication methods.

Number 7 (Page 20)

Chris Woolard discusses emergency regulation and learning from the coronavirus crisis

Number 8 (Page 21)

Covid-19 situation: BaFin information on new developments and key points

Number 9 (Page 22)

Written Testimony of L. Eric Patterson for a House Committee on Homeland Security hearing titled "Federal Protective Service: Ensuring the Mission is not Lost in Transition"

Number 10 (Page 26)

Long-range Communications without Large, Power-Hungry Antennas

Mosaic concept of distributed antenna “tiles” aims to transform tactical communications

Number 1

Financial system resilience - lessons from a real stress

Sir Jon Cunliffe, Deputy Governor for Financial Stability of the Bank of England, at the Investment Association Webinar, London.

The COVID 19 natural disaster has been the toughest test of the financial system since the global financial crisis 10 years ago.

As the implications of the spread of the virus and the policy measures to contain it became apparent, over a few short weeks, we saw an abrupt and savage pricing down of economic prospects and economic assets across the globe.

Investors, corporates, banks and households went into a defensive crouch, shunning risk, searching for safer havens, and stockpiling liquidity.

Many of the resultant moves were unprecedented. Bank lending surged as corporates drew down on their liquidity facilities.

In March, UK banks' net lending to corporates shot up to £33 billion, around 30 times the average monthly lending seen last year. The jump was even more striking in the US, where growth in the stock of corporate lending rose by over $600 billion in the first four months of the year, compared to an increase of less than $60 billion for 2019 as a whole.

In financial markets, the FTSE All-Share index fell over 10% on 12 March, the largest one-day fall since 1987. Some high-yield primary debt markets effectively closed: sterling issuance stopped on 13 February and US dollar issuance stopped on 4 March – and remained closed for longer than seen in the financial crisis. Even short-term funding markets for corporates, such as the commercial paper markets, became strained.

Initially, yields on risk-free assets fell rapidly at the end of February and early March due to the flight to safety. However, this became an abrupt and disruptive "dash for cash" in mid-March as investors demand for cash and near-cash assets rose sharply, resulting in selling pressure on usually safe and liquid assets such as government bonds. Risk free yields began to rise sharply and the financial conditions facing major economies tightened.

The “dash for cash” also spread to foreign exchange markets, given the dollar’s pivotal role in global trade and investment. US dollar funding became particularly difficult to raise in global capital markets; the dollar appreciated sharply; and FX liquidity deteriorated across all currency pairs as the near one-way demand for dollars drove bid-offer spreads up to three times their normal levels.

Central banks had to take extraordinary action to stabilise markets. In the UK, the MPC increased the stock of asset purchases by £200 billion to a total of £645 billion, and bought gilts at the fastest rate operationally possible.

These gilt purchases - equivalent to nearly a tenth of UK GDP - increased the supply of ‘cash’, reducing market interest rates, and improving liquidity in the gilt market.

In the US, the Fed initially announced it would purchase $500 billion in Treasuries, then removed the cap, moving to an open-ended purchase programme.

In the euro area, the ECB launched a €750 billion Pandemic Emergency Purchase Programme in March.

Over the past decade, asset purchases by central banks have become an established monetary policy tool to support demand. But in this instance, central banks were clear that their actions were aimed primarily at stabilising markets and preventing financial conditions tightening at the very time that economies needed the exact opposite.

As a result of these central bank interventions, and as fiscal authorities began to provide support to economies entering lockdown, conditions stabilised.

Non-financial investment-grade corporate bond spreads are now over 90 basis point lower than their peak in mid-March (but still around 40 basis points higher than their end-2019 levels).

The COVID crisis is very far from over. The depth and length of its economic impact remain very uncertain: it is clear that there is likely to be a great deal of pain for the financial sector.

Given the economic hit – a very deep synchronised hit to the global economy – we can expect very significant losses on credit to firms and households.

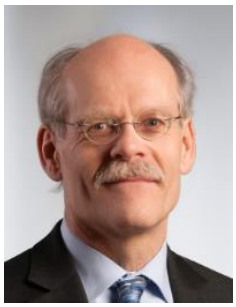
And future news about the health crisis and consequent policy measures or about geo-political tension, could well spark another very sharp repricing of economic prospects and financial assets.

To read more: https://www.bis.org/review/r200610a.pdf

Number 2

The monetary policy toolbox

Stefan Ingves, Governor of the Sveriges Riksbank, at the Swedish Economics Association, Stockholm.



The spread of the coronavirus came as an unpleasant surprise to us all. It is now clear that the economic consequences of the pandemic threaten to be both serious and protracted.

Most analysts have very weak forecasts for economic developments in the coming quarters, and in some scenarios also for a longer period to come.

We are in the midst of an unforeseen economic development that needs to be met with various macroeconomic tools, and the Riksbank has an important role to play here, together with the Government, the Riksdag (Swedish parliament) and other authorities.

During the initial phase of the crisis, we Executive Board members have already taken a large number of decisions to support the Swedish economy, and thus contribute to meeting the targets for economic policy, and I will comment on what we have done in more detail later on.

We can note that many of the measures have major consequences for the Riksbank's balance sheet – something that will be a recurring theme in today's speech.

Today I intend to focus primarily on how the "monetary policy toolbox" needs to look to be able to manage future challenges.

I will take a longer perspective and discuss which tools the Riksbank may need to use, especially if the low interest rate scenario that has characterised the past 10 years becomes even more prolonged.

The fact that monetary policy measures affect a central bank's balance sheet has become increasingly common in large parts of the world. This development has been driven by the very low interest rates and the need to make monetary policy even more expansionary.

Essentially, it is nothing new – if we go back in time, there are many examples of central banks that have used variation in their asset portfolios as a means of conducting monetary policy.

The monetary policy toolbox also needs to take into account changes in the financial system; for instance, we in Sweden have, in recent years, seen a development towards a higher share of market financing for Swedish companies.

As things look now, there is considerable probability that global interest rates will remain low over a long period of time, and then monetary policy will have to find other ways of working to attain the inflation target than those we are used to, and many of the measures will have consequences for the balance sheet.

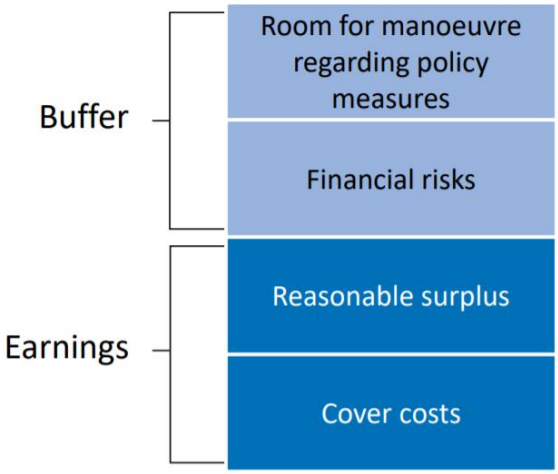
We need to endeavour to attain a better analysis of how measures that have an effect through the balance sheet affect the economy and become as clear and systematic when we talk about these as we have tried to be with regard to steering interest rates.

I intend to begin with a historical retrospective – focusing on the past 30 years – and to describe how monetary policy has developed over time.

Then I will move on to the challenges that monetary policy has faced and that have led to the use of new tools.

This takes me to the international discussions about the monetary policy toolbox, and, in conclusion, I would like to discuss what opportunities and limitations the Riksbank Inquiry's proposed new act entails.

Four reasons for holding equity capital



The international monetary policy discussion

Tried & tested monetary policy measures

Raised inflation target for greater monetary policy scope for action	Quantitative easing as a permanent part of the monetary policy toolbox
Make-up strategies for better "automatic stabilisation" of shocks	Forward guidance to influence expectations of future interest rates

To read more: https://www.bis.org/review/r200611c.pdf

The slides: https://www.bis.org/review/r200611c_slides.pdf

Number 3

COVID-19, The Pandemic and its Impact on Security Policy

Colonel Professor Dr. Matthias Rogg, Head of the German Institute for Defence and Strategic Studies (GIDS). PRISM is the quarterly journal of complex operations published at National Defense University (NDU).

The world is caught up in an existential struggle. The opponent is intangible; it spares neither state nor social group and does not stop at any border. For many of us, this struggle feels like war.

Indeed, with the growing use of war-like language in the fight against COVID-19, also called coronavirus, a rapidly rising number of victims, and last but not least the economic consequences which are becoming increasingly clear, we seem to be experiencing a war-like situation.

This includes the more and more apparent social and psychological effects of the crisis: An increasing uncertainty among large social groups, but also a strengthening of group cohesion.

People are afraid and join forces, but they also tend to be egoistic—certainly when their own livelihood is at risk—as illustrated by the EU member states' initial responses to the pleas of Italy and Spain.

Currently, attention is focused on two areas; the medical and the social domain, with the latter including legal, economic, political, and cultural aspects.

In view of the existential nature of the threat and the great uncertainties arising from the coronavirus crisis as well as the tensions that come with them, it is only a matter of time before this crisis also becomes the focus of security policy.

Germany's armed forces are already making a significant effort to deal with the COVID-19 outbreak. To address the coronavirus crisis, the Bundeswehr (the German Armed Forces) has mobilized 15,000 soldiers within a very short time, has set up four regional commands to facilitate coordination, has supported interagency action when it comes to procurement processes, and has organised further activities with creative ideas (e.g. by making use of the "Helping Hands" concept).

The Bundeswehr has a long tradition of providing subsidiary assistance in

emergency situations, which ranges from procurement and logistical support to area and facility protection by performing tasks in support of law enforcement and traffic control.

Operations during an epidemic are nothing new to the Bundeswehr as shown most recently in the fight against Ebola in 2014 and 2015.

What is new, however, is the scale and the speed with which states and societies around the world are being hit hard by the current crisis.

Pandemic Risks Have Been Known

The existential threat of a pandemic has always been a matter of public safety and security policy in Germany.

The outbreak of the highly pathogenic Marburg virus in 1967 is just one example. As part of a notification provided by the Federal Government, an extensive chapter of the 2012 report on risk analysis in civil protection discusses a pandemic due to a “Modi-SARS virus.”

In view of current events, this chapter reads like an ominous and all too accurate warning.

In the current version of the White Paper on German Security Policy and the Future of the Bundeswehr published in 2016, a short section entitled “Epidemics and Pandemics” links the risks of regional destabilisation to systemic risks (which may also emerge in our country) and to Germany’s interest in and responsibility for prevention and crisis management in cooperation with international partners and organisations.

In 2015, the Helmut Schmidt University/ Bundeswehr University Hamburg, on behalf of the Bundeswehr Office for Defence Planning, applied methods from the field of mathematics to compare different operations and research models that can be used to predict the course of an epidemic in a theater of operations.

With regard to Africa, a dual strategy characterised by significantly improved infrastructure and early detection seemed to be the most promising.

The Bundeswehr, together with NATO partner states, is already using disease surveillance systems such as ASTER to ensure the rapid detection of infectious disease outbreaks.

To improve the infrastructure, the “One Million Community Health Workers” campaign, which was launched in 2013 and aims at employing one million community health workers in Africa, could be further developed.

You can read more at page 55:
https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-4/prism_8-4.pdf

Number 4

PCAOB Announces Webinar for Audit Committee Members

PCAOB
Public Company Accounting Oversight Board

The Public Company Accounting Oversight Board (PCAOB) has announced that it will host a webinar for audit committee members at 2 pm on *Wednesday, July 8*.

"Audit committees are on the front lines of promoting audit quality, which is why one of the Board's strategic priorities is to interact more often and more directly with them," said Chairman William D. Duhnke.

"This webinar for audit committee members is a first for the PCAOB, and we look forward to the opportunity to further engage."

The session will provide an overview of:

- the PCAOB's new inspection reports;
- auditing and inspecting audits in the COVID-19 environment;
- new and recent auditing standards activity (e.g., estimates, specialists, critical audit matters, and systems of quality control);
- data and technology; and
- audience Q&A.

Speakers will include PCAOB Chairman Duhnke, Chief Auditor Megan Zietsman, Deputy Director of Inspections Christina Gunia, and Stakeholder Liaison Erin Dwyer.

The webinar is open to public company audit committee members. There is no fee to attend, but advanced registration is required. Please email the PCAOB's stakeholder liaison Erin Dwyer at dwyere@pcaobus.org for registration instructions.

Number 5

The European Central Bank's policy in the COVID-19 crisis - a medium-term perspective

Isabel Schnabel, Member of the Executive Board of the European Central Bank, at an online seminar hosted by the Florence School of Banking & Finance, Frankfurt am Main.

Over the past few weeks, hopes for a short duration of the COVID-19 pandemic and a quick rebound in economic activity have started to fade.

Evidence is increasingly pointing towards a protracted impact of the crisis on both demand and supply conditions in the euro area and beyond.

For central banks, this implies a shift in focus from economic "firefighting" – ensuring orderly market functioning and a sufficient provision of liquidity – to dealing with the implications of the crisis on medium-term inflation.

My remarks today will focus on these implications.

Based on our most recent Eurosystem staff projections, I will first discuss the risk of COVID-19 leaving a deep footprint on growth and inflation in the euro area.

Against this background, I will then describe how we designed and calibrated our policy response, and explain why the pandemic emergency purchase programme (PEPP) remains the appropriate tool to address the current challenges of the crisis in the context of our price stability mandate.

The medium-termeconomic impact of the crisis

The immediate economic fallout from the COVID-19 pandemic has been substantial.

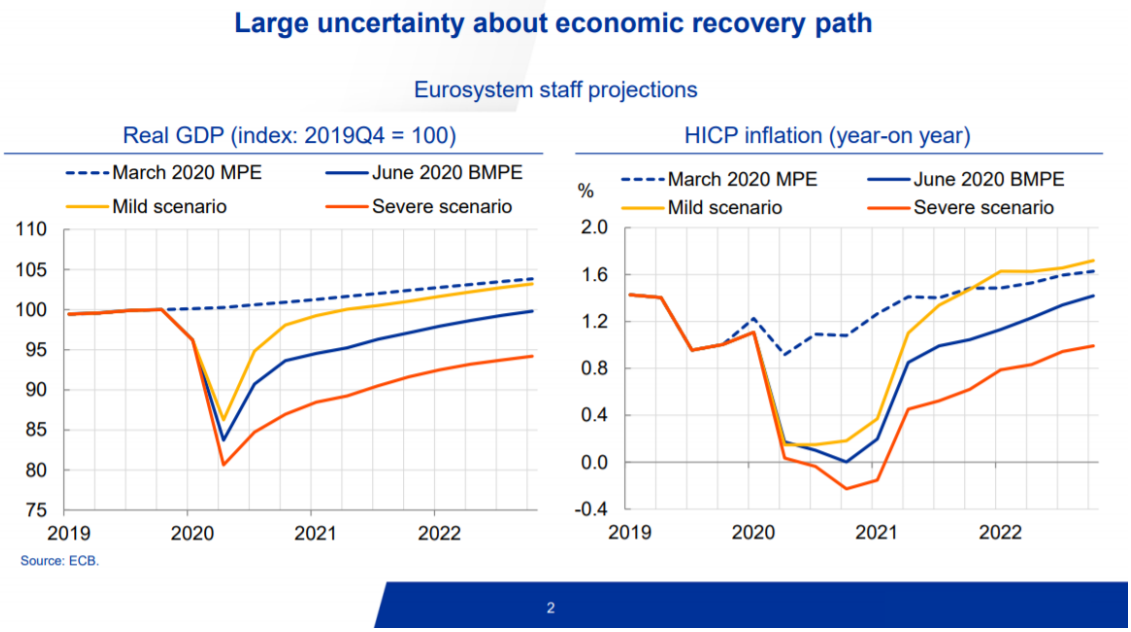
In the first quarter of 2020, euro area GDP declined by 3.6%.

In the baseline scenario of the Eurosystem June staff projections, output declines by a staggering 13% quarter-on-quarter in the second quarter.

As lockdown measures are being eased across euro area countries, a cautious recovery in activity is currently taking place.

But adverse effects on household income and production can be expected to persist for a considerable period of time.

Such protracted effects are clearly visible in the most recent Eurosystem staff projections.



Given the current exceptional degree of uncertainty, these projections were organised around three scenarios that differ with respect to the severity of the economic fallout from the pandemic in the euro area (see left chart on Slide 2).

All scenarios assume that the substantial support from monetary, fiscal and labour market policies is sufficient to avert adverse financial amplification channels.

While the severity of the contraction differs substantially across scenarios, none of the three trajectories is in line with a full recovery of real GDP by the end of 2022 to the levels projected by staff in March.

In the severe scenario, our staff projections suggest that the level of real GDP at the end of 2022 could remain 9.6% below the March 2020 staff projection path.
In effect, both the nature of the shock and the length of the ensuing downturn make it likely that the economy will experience important structural shifts.

Disentangling the effects of these shifts on demand and supply, and hence on medium-term inflation, is inherently difficult.

To read more: https://www.bis.org/review/r200611a.pdf

The slides: https://www.bis.org/review/r200611a_slides.pdf

Number 6

Tips for secure user authentication

In an era of large-scale data breaches, The European Union Agency for Cybersecurity shares its recommendations for improving the security of passwords and authentication methods.

We are living in an era of large-scale data breaches. More and more high-profile companies are hacked; as a result, the personal data of millions of customers is leaked online.

Cybercriminals with different motivations and interests take advantage of this data in order to mount attacks at both individuals and other organizations.

As passwords are still the main method to authenticate users to platforms and systems, this article aims to provide tailored recommendations for improved cyber hygiene.

Risks to passwords

Today, passwords can be stolen in multiple ways, including:

1. Social Engineering attacks such as phishing credentials using fake pages, voice phishing (so-called Vishing), shoulder surfing (e.g. peeping behind a person who is typing their password on a laptop) and even retrieving handwritten passwords from post-it notes.

2. Stealing using specialized software or physical keyloggers. Some of these attacks require a physical presence or proximity to a laptop or a device.

3. By intercepting communications, using fake access points or by leveraging man-in-the-middle attacks (MiTM) at a network level, more prevalent in public WiFis found in hotels, cafés, airports, etc.

4. Brute-force attacks on passwords by trying all the combinations, dictionary attacks or by simply guessing the password.

5. Retrieving passwords directly from data breaches and leveraging them using password spraying techniques to other legitimate services.

Recommendations to improve password security

1. Activate multifactor authentication functionality whenever possible for all of your accounts.

2. Do not re-use your passwords. Cybercriminals work under the assumption that many users re-use passwords, hence their high success rates for compromising accounts.

3. Use single sign-on functionality combined with multifactor authentication in order to reduce the risk of account compromise.

4. Use a password manager.

5. Generate strong and unique passwords or passphrases according to the latest guidelines available, for each individual website and service. This is where password managers come in handy.

6. Check if any your accounts appear in existing data breaches and act immediately by changing your passwords for the services identified.

7. Many websites offer password reminder functionalities. Make sure you do not rely on easily retrievable personal information to reset your password, e.g. name of your pet, your date of birth, your high school, etc.

8. Make use of VPNs or at least mobile access points when accessing e-Banking or other private services from public WiFi.

9. Be aware of your surroundings in lounges, airports, trains and cafés, and make sure there is nobody behind you trying to snoop your password. This is where screen privacy filters come in handy.

10. Do not leave your devices unattended/unlocked in public spaces such as hotels, public transport, lounges, etc.

For more security awareness related materials, please visit the website of the European Cyber Security Month (ECSM) awareness raising activity coordinated by ENISA at:
https://cybersecuritymonth.eu/references/partners-resources/resources#c7=effective&reversed=on&b_start=0

Number 7

Chris Woolard discusses emergency regulation and learning from the coronavirus crisis

In his first Inside FCA podcast interview, Interim Chief Executive Chris Woolard discusses how the FCA has rapidly reprioritised work in light of the coronavirus (Covid-19) pandemic, and talks about future business planning

In the interview Chris Woolard talks about the FCA's work to reduce economic impact while helping to protect consumers, outlining the regulatory approach to recent crisis planning.

“What we’ve wanted to do is to get the firms we regulate to focus on serving their consumers through what’s a very difficult time, and also in particular looking at those who are vulnerable.”

He then explains specific areas of intervention, including mortgages and Business Interruption (BI) insurance, before talking in detail about the challenges and opportunities of technological advancement from new players in the financial services markets.

Addressing the priorities in the Business Plan, he lays out ‘clear areas of real focus’ as part of ongoing work, including retail investments, payments and protections for the consumer credit market.

He ends by talking about how recent crisis planning should be used to help with future work:

“I think one of the big lessons from the crisis is that importance of timely rapid information that really allows you in a matter of hours to assemble a picture on a market or a series of firms has been absolutely vital where we have it.

And that’s something that I think we should have uniformly across every single market that we regulate, and we should make full use of it to deliver a better public service.”

The podcast (22 minutes) at:
https://www.fca.org.uk/media/podcast/inside-fca-podcast-chris-woolard-interview-emergency-regulation-and-future-planning

Number 8

Covid-19 situation: BaFin information on new developments and key points

BaFin Federal Financial Supervisory Authority

Due to the special situation surrounding COVID-19 (the novel coronavirus), BaFin has been receiving numerous queries from associations and institutions, many of which allude to the same topics.

In the following, BaFin consolidates and responds to these queries. Where applicable, these explanations, which are provided by BaFin's Banking Supervision Sector, apply mutatis mutandis to securities trading banks and financial services institutions (leasing and factoring companies).

Any questions in this regard should be directed to the securities supervision division responsible for your institution.

This is a living document that is being updated and supplemented on an ongoing basis.

BaFin welcomes additional suggestions and will soon be taking these into account in this list.

To read more:
https://www.bafin.de/EN/Aufsicht/CoronaVirus/CoronaVirus_node_en.html

Number 9

Written Testimony of L. Eric Patterson for a House Committee on Homeland Security hearing titled "Federal Protective Service: Ensuring the Mission is not Lost in Transition"

Good afternoon Chairwoman Torres Small, Ranking Member Crenshaw, and Members of the Subcommittee. Thank you for the opportunity to testify today on behalf of the U.S. Department of Homeland Security's (DHS) Federal Protective Service (FPS) regarding FPS's critical mission within DHS.

In the year 2021, FPS will celebrate its 50th anniversary. Since its inception in 1971, FPS has protected people and property in the Federal government by identifying and mitigating vulnerabilities through risk assessments, law enforcement, intelligence analysis, and security countermeasures.

Today, we protect over 9,000 facilities and more than 1.4 million people who work, visit, or conduct business at these facilities each day.

FPS provides the DHS Secretary with a highly trained, nationwide force that can support the Department's mission in countering emerging or existing threats and terrorism, within the boundaries of our Nation and territories.

Each day, tens of thousands of law enforcement officers, including the officers of FPS, risk their lives in protecting and securing this great nation. In recognition of their sacrifices, nearly one month ago, citizens across the United States came together to participate in National Police Week to honor and remember our fallen law enforcement officers.

In its history, FPS has had six sworn officers killed in the performance of their duties.

This serves as a sobering reminder that the women and men of FPS must remain vigilant and well-prepared to prevent, protect, respond to and recover from events that threaten our nation's people, property, and institutions.

FPS Overview

FPS was established in 1971 as the uniformed protection force of the General Services Administration (GSA). On March 1, 2003, pursuant to the Homeland Security Act of 2002 (6 U.S.C. §§101 et. seq), FPS was transferred from GSA to DHS in recognition of the role FPS plays in securing our homeland.

At the time, it was placed within U.S. Immigration and Customs Enforcement, but found a more permanent home in 2009 with the National Protection and Programs Directorate which was being established at that time.

Headquartered in Washington DC, FPS is organized through three Zones and 11 Regions for mission execution.

FPS Workforce

The skills, talents, and dedication of our workforce form the foundation of our success.

Our workforce of nearly 1,400 federal personnel is comprised of approximately 1,000 law enforcement officers and 400 mission support staff. In addition to contract staff augmentation, FPS contracts for approximately 14,000 security guards, more appropriately known as Protective Security Officers (PSOs).

Our law enforcement personnel – inspectors, police officers, and special agents – are employed throughout the Nation and our Nation's territories. They are trained physical security experts and sworn Federal law enforcement officers.

Our law enforcement personnel perform a variety of critical functions, including conducting comprehensive security assessments to identify vulnerabilities at federal facilities, developing and implementing protective countermeasures, providing uniformed police response and investigative follow-up to crimes and threats, and other law enforcement activities in support of our mission.

In addition to FPS's law enforcement officers, FPS also employs nearly 400 mission support staff who are responsible for a myriad of important tasks within the organization including outreach and engagement with critical external stakeholders (e.g. Congress and the Federal Executive Boards); human capital management; finance, budgeting, and performance; and, law enforcement and security training.

FPS, through contracts with commercial security vendors, utilizes approximately 14,000 PSOs, to assist in the protection of Federal facilities. Our contracted PSOs are often the front line of FPS and are in daily contact with our Federal facility customers and visitors.

They too put themselves at risk to accomplish our mission, to include making the ultimate sacrifice. During my tenure here at FPS, I have attended the funerals of two of our contract PSOs who were killed standing watch.

FPS Authorities

FPS law enforcement personnel derive their law enforcement authority and powers from section 1706 of the Homeland Security Act of 2002, codified in 40 U.S.C. § 1315. Pursuant to this authority, the Secretary of Homeland Security can designate law enforcement personnel for the purposes of protecting property owned or occupied by the Federal Government and persons on that property.

These designated law enforcement personnel have specific statutorily-prescribed police powers, to include enforcing Federal laws and regulations, carrying firearms, making arrests, conducting investigations, and serving warrants and subpoenas issued under the authority of the United States.

Specifically, 1315-designated officers may conduct investigations of offenses that may have been committed against either property owned or occupied by the Federal Government, or persons on such property, and make arrests without a warrant for any offense against the United States committed in the presence of the officer or for any felony cognizable under the laws of the United States if the officer or agent has reasonable grounds to believe that the person to be arrested has committed or is committing a felony.

On February 18, 2005, the U.S. Attorney General approved Guidelines for The Exercise Of Law Enforcement Authorities By Officers And Agents Of the Department Of Homeland Security as required in 40 U.S.C. § 1315(f). These approved Guidelines govern the exercise of the law enforcement powers of DHS officers designated by the Secretary under 1315(b)(1).

Additionally, consistent with 41 C.F.R. § 102-85.35, FPS Law Enforcement Personnel provide general law enforcement services on GSA property, and per 41 C.F.R. § 102-74.15, all occupants of facilities under the control of Federal agencies must promptly report all crimes and suspicious activities to FPS.

Most recently with the passage of the Preventing Emerging Threats Act of 2018, codified at 6 U.S.C. 124n, FPS and its organic statute, 40 U.S.C. § 1315, is an integral part of the Department's development and use of security countermeasures for unmanned aircraft systems (UAS) that threaten the security of federal facilities and persons thereon.

The Department, under the law enforcement and security provisions found in 40 U.S.C. § 1315, is authorized to use certain UAS countermeasures for protection of federal facilities.

FPS Funding Structure – New Fee Model

FPS collects fees from federal departments and agencies in order to execute its mission throughout our Nation and territories with a total budget authority of $1.6B in FY 2019. We derive our funding through the collection of fees from our tenant customers (the Federal government) based on a square-footage model in which we charge $0.78 per square foot of those facilities we protect and secure and eight- percent overhead on PSO and Technical Counter Measure (TCM) contracts.

However, beginning in Fiscal Year (FY) 2020, FPS is employing a risk-based revenue model to better align basic security assessments to the security work that FPS performs. The new approach employs statistical analysis of operational workload data at each building to understand the key drivers of FPS's security costs.

FPS uses the model that the analysis produces to determine the basic security assessments for each customer agency. All told, this approach offers a more equitable method for assessing basic security fees because it reflects FPS's historical security workload data for each building.

Using historical workload data, this new revenue model is security oriented whereas the square- footage model represented a rent-based approach that did not accurately reflect the law enforcement and security work FPS executes daily.

To read more:
https://www.dhs.gov/news/2019/06/11/written-testimony-l-eric-patterson-house-committee-homeland-security-hearing-titled

Number 10

Long-range Communications without Large, Power-Hungry Antennas

Mosaic concept of distributed antenna "tiles" aims to transform tactical communications

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Establishing long-range tactical communications for U.S. troops in remote locations currently requires giant parabolic dishes, tall pole-mounted antennas, large antenna domes, and high-power amplifiers.

Besides their significant weight, power, and cost (SWAP-C), these antennas present large visual and radio frequency (RF) signatures, are vulnerable to jamming, and constitute a single point of failure.

To break this dependence on big antennas and amplifiers, DARPA recently announced the *Resilient Networked Distributed Mosaic Communications (RN DMC)* program.

RN DMC aims to provide long-range communications through "mosaic" antennas composed of spatially distributed low SWaP-C transceiver elements or "tiles."

This approach replaces high-powered amplifiers and large directional antennas with mosaics of dispersed tile transceivers.

Transmit power is distributed among the tiles, and gain is achieved through signal processing rather than by a physical antenna aperture to concentrate energy.

"This is a fundamentally different way to think about long-range tactical communications that supports DARPA's Mosaic Warfare concept of busting monolithic systems and distributing capability for greater resilience at less expense," said Paul Zablocky, program manager in DARPA's Strategic Technology Office.

"RN DMC seeks to develop a mobile, self-forming, self-healing mosaic antenna comprising numerous low-cost and low-power transceiver tiles that can be placed aboard ships, vehicles, unmanned and manned aircraft, and satellites, as well as individual squad members."

The antenna mosaic concept could prove more robust against failure or attack since tiles are distributed across air, ground, and sea assets.

Tiles also promise to be lower cost – targeted at $1,000 or less apiece – making individual tiles expendable without losing the mosaic antenna functionality.

“Powerful signal processing in a small, inexpensive form factor is the key enabling mosaic antenna technology,” Zablocky said. “We will leverage small form factor software-defined radios and radio frequency systems on a chip as well as previous DARPA research and development efforts that have validated the feasibility of basic distributed coherent radio transmissions.”

RN DMC includes three focus areas: system design, experimental performance validation, and operational architecture definition. The effort is divided into three planned phases, totaling 45 months.

A Broad Agency Announcement solicitation with full program details is available here: https://go.usa.gov/xw9PK

A Proposers Day webinar has been scheduled for June 29. For more information and registration details, visit: https://go.usa.gov/xwWCY

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.

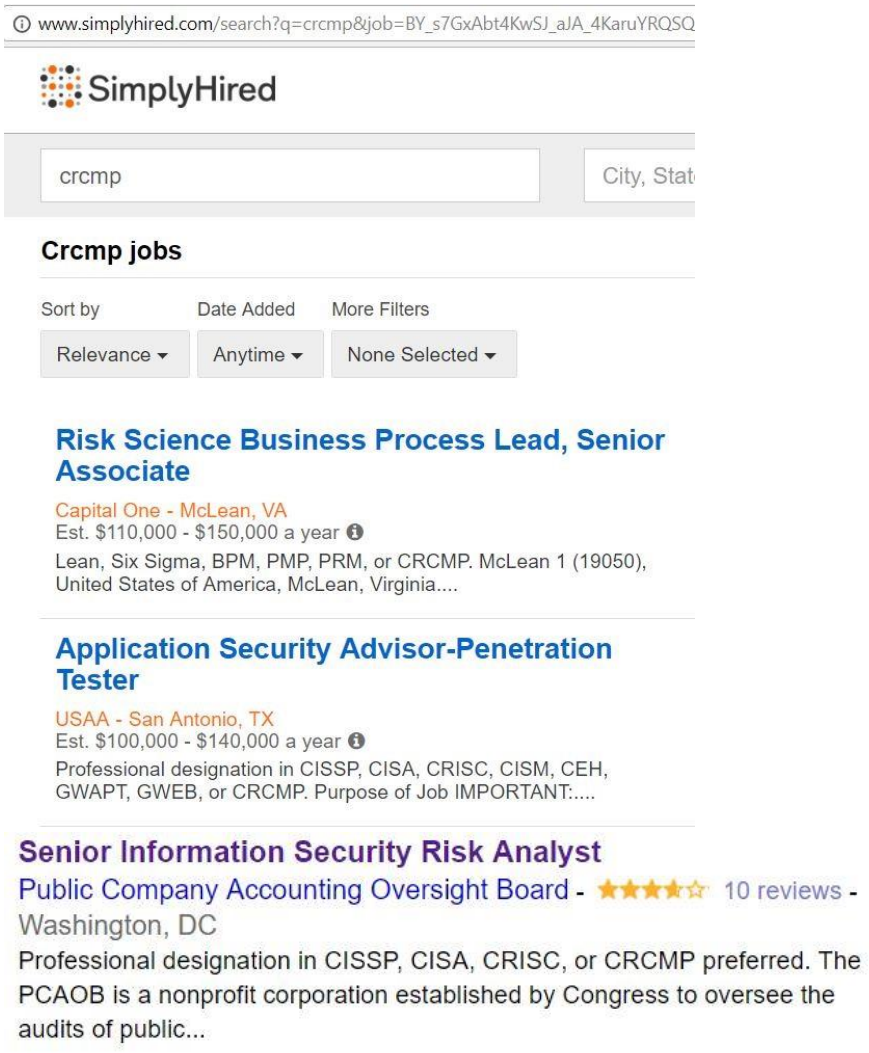
International Association of Risk and Compliance Professionals

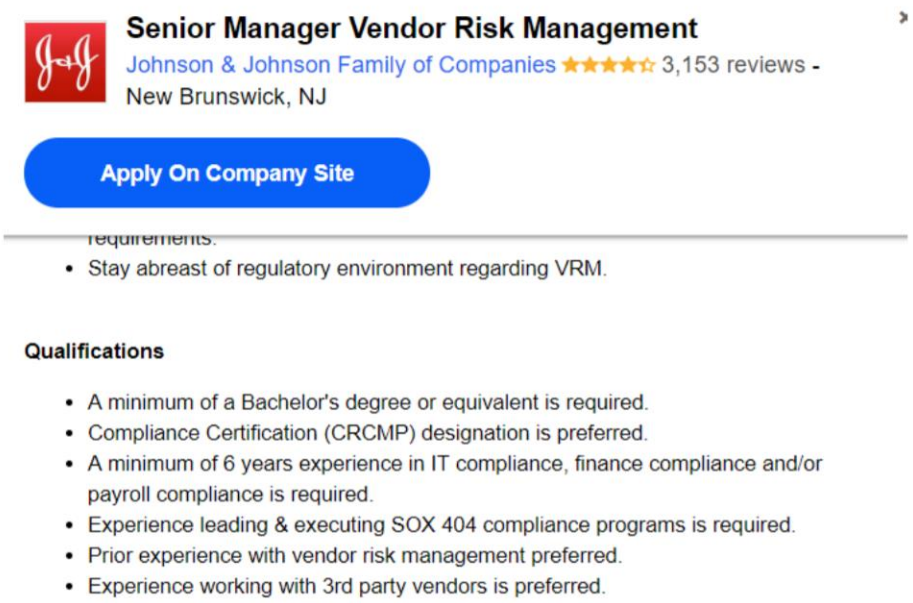
You can explore what we offer to our members:

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