Monday, June 1, 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,

According to the European Insurance and Occupational Pensions Authority's (EIOPA) updated Risk Dashboard, *macro risks* increased from high to very high given the global impact of the outbreak of COVID on economic activities.

GDP growth forecasts have been *revised significantly* downwards for all geographical areas, while inflation is expected to decrease slightly.

The indicator on the 10-year swap rates decreased reaching new lows, after a flattening of all swap curves on the long end.

Monetary support has been activated by all major central banks.

Credit risks increased to high level. The most recent market data signal a spike in credit risks across all market segments.

CDS spreads of financial and non-financial bonds show the highest increase. Government bond CDSs increased overall across countries, with heterogeneity in magnitude within the EU.

The median average quality of insurers' investments remained stable to levels between AA and A for Q4-2019.

Market risks increased from high to very high level during March 2020.

Covid-19 impacts on financial markets has been strong: volatilities both in bond and equity markets have increased. *Global equity prices* fell by over 30%, with expected deterioration of insurers' equity investment by a similar magnitude.

Flight to quality investment behaviors and increase of risk premia put downward pressure also on corporate and sovereign bond prices, resulting in overall expected decrease in insurers' bond valuations.

There is heterogeneity across countries, some of which experienced substantial increase in sovereign yield spreads.

Liquidity and funding risks increased to high level, as some indicators are expected to worsen via the latest market developments and the strong hit on economic activities, which is reducing incomes and could result in decreasing premiums and lowering new business.

Moreover, the potential increase in certain claims and illiquid level of certain assets could put additional strains on the disposable liquidity of insurers in a medium to long-term horizon.

On the other hand, the two indicators on asset liquidity – cash holdings and liquid assets ratio – show minor increases in the median value in Q4 2019.

Volumes of bonds issued by insurance groups decreased. Catastrophe bond issuance increased, with the large majority of cat bonds issued covering US earthquakes risks.

Profitability and solvency risks increased to high level. A worsening of indicators is expected as a consequence of the negative recent market developments in the context of Covid-19 outbreak.

Furthermore, a decrease on excess of assets over liabilities is expected, driven by drops in asset values and increase in liabilities.

On the other hand, Solvency II data for Q4-2019 displayed a deterioration of the net combined ratio and return on premiums, while a significant increase of SCR ratios for insurance groups and life solo undertakings was observed.

This raise is mainly explained by a substantial increase in eligible own funds in France, as a result of a legislative change. Furthermore, an improvement of SCR ratios is observed for several solo life and groups undertakings in comparison with the previous quarter due the increase on the risk free curve in Q4 2019.

Insurance risks increased to high level. The negative market developments may have negative effects via income reduction (due to the impact of drop in economic activity on new as well as existing business) and potential increase in claims for specific business lines.

On the other hand, median premium growth for both, life and non-life business, remains positive in Q4 2019, with an observed deterioration for life business.

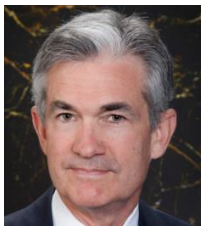
The catastrophe loss ratio of main reinsurers increased following the most significant events of 2019 in terms of insured losses – Typhoon Hagibis, which hit Japan in mid-October.

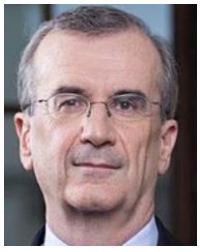
Read more at number 6 below. Welcome to the Top 10 list.

Best regards,

George Lekatis

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





A transformative, cloud-computing approach to analyzing data helps researchers better understand seismic activity

Los Alamos National Laboratory
Delivering science and technology to protect our nation and promote world stability

Number 6 (Page 19)

European insurers face increased risk exposures due to Covid-19, but market perceptions and imbalances remained at medium level

eiopa
European Insurance and Occupational Pensions Authority

Number 7 (Page 22)

Actions Needed to Enhance DHS Oversight of Cybersecurity at High-Risk Chemical Facilities

United States Government Accountability Office
GAO
Report to Congressional Requesters

Number 8 (Page 24)

Data and Technology Research Project Update Spotlight

PCAOB
Public Company Accounting Oversight Board

Number 9 (Page 25)

The BIS at 90

BIS

Number 10 (Page 27)

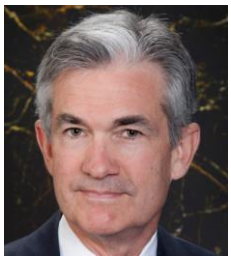
Notice of cyber security incident

easyJet plc

Number 1

Coronavirus and CARES Act

Testimony by Mr Jerome H Powell, Chair of the Board of Governors of the Federal Reserve System, before the Committee on Banking, Housing, and Urban Affairs, US Senate, Washington DC.



Chairman Crapo, Ranking Member Brown, and other members of the Committee, thank you for the opportunity to discuss the extraordinary steps the Federal Reserve has taken to address the challenges we are facing.

I would like to begin by acknowledging the tragic loss and tremendous hardship that people are experiencing both here in the United States and around the world.

The coronavirus outbreak is, first and foremost, a public health crisis, with the most important responses coming from those on the front lines in hospitals, emergency services, and care facilities.

On behalf of the Federal Reserve, let me express our sincere gratitude to those individuals who put themselves at risk day after day in service to others and to our nation.

The forceful measures that we, as a country, are taking to control the spread of the virus have substantially limited many kinds of economic activity. Many businesses remain closed, people have been advised to stay home, and basic social interactions have been greatly curtailed.

People have put their lives and livelihoods on hold at significant economic and personal cost. All of us are affected, but the burdens are falling most heavily on those least able to carry them.

It is worth remembering that the measures taken to contain the virus represent an investment in our individual and collective health. As a society, we should do everything we can to provide relief to those who are suffering for the public good.

Available economic data for the current quarter show a sharp drop in output and an equally sharp rise in unemployment.

By these measures and many others, the scope and speed of this downturn are without modern precedent and are significantly worse than any recession since World War II.

Since the pandemic arrived in force just two months ago, more than 20 million people have lost their jobs, reversing nearly 10 years of job gains. This precipitous drop in economic activity has caused a level of pain that is hard to capture in words, as lives are upended amid great uncertainty about the future.

In addition to the economic disruptions, the virus has created tremendous strains in some essential financial markets and impaired the flow of credit in the economy.

The Federal Reserve's response to this extraordinary period has been guided by our mandate to promote maximum employment and stable prices for the American people, along with our responsibilities to promote stability of the financial system.

We are committed to using our full range of tools to support the economy in this challenging time even as we recognize that these actions are only a part of a broader public-sector response.

Congress's passage of the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) was critical in enabling the Federal Reserve and the Treasury Department to establish many of the lending programs that I discuss below.

In discussing the actions we have taken, I will begin with monetary policy.

In March, we lowered our policy interest rate to near zero, and we expect to maintain interest rates at this level until we are confident that the economy has weathered recent events and is on track to achieve our maximum - employment and price-stability goals.

In addition to monetary policy, we took forceful measures in four areas: open market operations to restore market functioning; actions to improve liquidity conditions in short-term funding markets; programs in coordination with the Treasury Department to facilitate more directly the flow of credit to households, businesses, and state and local governments; and measures to allow and encourage banks to use their substantial capital and liquidity levels built up over the past decade to support the economy during this difficult time.

Let me now turn to our open market operations and the circumstances that necessitated them.

As tensions and uncertainty rose in mid-March, investors moved rapidly toward cash and shorter-term government securities, and the markets for Treasury securities and agency mortgage-backed securities, or MBS, started to experience strains.

These markets are critical to the overall functioning of the financial system and to the transmission of monetary policy to the broader economy.

In response, the Federal Open Market Committee undertook purchases of Treasury securities and agency MBS in the amounts needed to support smooth market functioning. With these purchases, market conditions improved substantially, and thus we have slowed our pace of purchases.

While the primary purpose of these open market operations is to preserve smooth market functioning and effective policy transmission, the purchases will also foster more accommodative financial conditions.

As a more adverse outlook for the economy associated with COVID-19 took hold, investors exhibited greater risk aversion and pulled away from longer-term and riskier assets as well as from some money market mutual funds.

To help stabilize short-term funding markets, we lengthened the term and lowered the rate on discount window loans to depository institutions.

The Board also established, with the approval of the Treasury Department, the Primary Dealer Credit Facility (PDCF) under our emergency lending authority in section 13(3) of the Federal Reserve Act.

Under the PDCF, the Federal Reserve provides loans against good collateral to primary dealers that are critical intermediaries in short-term funding markets.

Similar to the largescale purchases of Treasury securities and agency MBS I mentioned earlier, this facility helps restore normal market functioning.

In addition, under section 13(3) and together with the Treasury Department, we set up the Commercial Paper Funding Facility, or CPFF, and the Money Market Mutual Fund Liquidity Facility, or MMLF.

Both of these facilities have equity provided by the Treasury Department to protect the Federal Reserve from losses.

Indicators of market functioning in commercial paper and other short-term funding markets improved substantially and rapid outflows from prime and tax-exempt money market funds stopped after the announcement and implementation of these facilities.

To read more:
https://www.bis.org/review/r200519a.pdf

Number 2

European solidarity put to the test by the health crisis

François Villeroy de Galhau, Governor of the Bank of France, at the digital conference at the Bocconi University, Milan.

Ladies and Gentlemen, cari professori e studenti,

I am delighted to share this moment with you. I would like to extend my warmest thanks to all of those who made this virtual meeting possible in particular Rector Gianmario Verona, and Vice-Rector Stefano Caselli together with Francesco Daveri.

To me, Bocconi represents a major source of influence for European integration. Think of some great "bocconiani" who played a fundamental role in building our Economic union: from Luigi Einaudi – the father of the fathers of Europe – to my friend Mario Monti.

I also want to honour the memory of Tommaso Padoa-Schioppa who passed away ten years ago. In the difficult times we are facing, his vision and ability to translate European ideals into active fights – such as the euro – remain inspirational.

Today I stand before you as a committed European, a central banker, but also a friend of Italy. I first and foremost want to express my deep solidarity: Italy – like France – has been one of the countries hardest hit by the pandemic.

I am also well aware of the criticism about Europe being too slow or reluctant to help.

So my purpose today is a challenging one, as I will address the issue of Europe's alleged lack of solidarity.

I will first argue that in fact Europe – and the Eurosystem at the frontline – has broadly risen to the challenge during this acute phase of the crisis.

But we need to do more, and I will then sketch the broad outlines of an effective and collective exit strategy.

I. The Eurosystem at the front line of the European response during the acute phase of the crisis

The lockdown measures have a major impact on the European and so on the Italian economy, which – according to the European Commission – could contract by 9.5% in 2020.

Confronted with this unprecedented and totally unforeseen crisis, the policy response of European Governments – including Italy's – was immediate and strong.

But on both sides of our borders, there is a common temptation to blame Europe for not doing enough.

In reality, Europe is taking action, and more than has been acknowledged. The debate on "Coronabonds" has divided Europeans, but the exceptional monetary action taken by the European Central Bank (ECB) – which is much more significant – should bring us together.

In order to fulfill its mandate, the Eurosystem has always been clear in its commitment to ensure appropriate financial conditions in all parts of the euro area, and decisive in its action to fight fragmentation within the euro area.

We will not allow adverse market dynamics to lead to unjustified interest rate increases in some countries, which would put at risk the smooth transmission of our common monetary policy.

To put it simply: yields and spreads do matter, even if we don't target fixed levels. Hence, and consistent with the risk of still lower inflation, we announced on 18 March a EUR 750 billion Pandemic Emergency Purchase Programme (PEPP).

In implementing the PEPP, we are and will remain flexible; the Eurosystem should be guided more by market dynamics and liquidity conditions than predetermined volumes of purchases.

To read more:
https://www.bis.org/review/r200515a.pdf

Number 3

Securing smart infrastructure during the COVID-19 pandemic

Securing smart homes and smart buildings from cybersecurity risks becomes more relevant than ever in the light of the COVID-19 pandemic crisis. ENISA presents some fundamental measures for securing smart devices.

The Internet of Things (IoT) has changed the way people live, do business, and interact. Buildings and homes are becoming smarter, more complex and more connected. This massive interconnection leads to new efficiencies and capabilities and unlocks enormous value for consumers, organizations and cities. Nevertheless, these advantages come with great challenges and cyber security risks.

Securing smart homes and smart buildings from cyber security risks becomes more relevant than ever in the light of the COVID-19 pandemic crisis. People are spending considerable time at home using smart cameras, wearables and telecommunications to remain in touch with their business, doctors, government, school, friends and family.

Utilizing modern technology people stay productive for their work and their housekeeping, but they also become more susceptible to attacks from threat actors that are still looking to cash in by exploiting human nature.

Securing the home

Social distancing has shifted daily habits with activities pertinent to work, education, healthcare, wellbeing and socialisation happening mainly from home. Most of these activities are taking place in digital format and therefore they rely heavily on connectivity and smart home devices.

Many consumers are aware that their smart devices could potentially introduce vulnerabilities in their home network and they should configure them properly.

However, they struggle to understand what is required of them to keep their smart thermostat or voice assistants secure.

Below, ENISA presents some fundamental measures for securing smart devices:

- Use long passwords, two-factor or multi-factor authentication and, if available, enable biometric features or additional PINs.

- Use different passwords for each device in your home network.

- Observe user guides and enable the relevant security features during the initial setup.

- Enable update notifications and perform updates on a regular basis

- Avoid introducing sensitive information and be aware of the way your information is used.

- Turn off and unplug the device when no longer used

- Configure multiple networks on your router and keep your smart devices on a separate Wi-Fi network.

- Securely wipe your smart device and use “factory reset” function before disposing or returning it back.

Securing the business premises

Almost overnight, in an effort of implementing immediately social distancing, many employees around the globe started working remotely from home and staying away from offices.

Outside of the normal and business-as-usual situation, with applying social distancing rules and personnel working in rotation, employees might simply be less diligent about security practices.

It has never been more important to proactively secure smart buildings/offices, which they often control systems or operations like data centers dependent on the availability of air conditioning systems.

Securing networks, monitoring network anomalies, identifying malicious behaviour including social engineering and spear phishing attempts and reviewing IoT security configurations is the way forward and in that respect, ENISA provides the following recommendations in addition to the ones mentioned above:

- Enable firewall protection, and ensure corporate network is only accessible from whitelisted services.

- Disable unused ports.

- Apply network micro-segmentation by creating virtual networks to isolate IoT systems from other critical IT systems.

- Enable monitoring and diagnostics and review them regularly.

- Prepare and update the incident response plans according to the current risks.

Smart homes and smart buildings have become the digital shelters for all people in social distancing. Securing them is a shared responsibility and everyone should take part in achieving a more secure and resilient digital environment both at home and at work.

Number 4

Mitigating Disinformation in Southeast Asian Elections: Lessons from Indonesia, Philippines and Thailand

Published by the NATO Strategic Communications Centre of Excellence

In 2019, a series of elections in the Southeast Asian countries of Indonesia, the Philippines, and Thailand highlighted the salience of digital media in political campaigns and insidious modes of electoral manipulation.

Despite new legal, technical, social, and educational efforts to mitigate "fake news," our comparative research analysis of elections in the three countries observes that digital disinformation has become further entrenched in electoral processes.

We observe that a wider range of political actors and parties enlisted a diversity of digital campaign specialists and paid out "buzzers" (Indonesia), "trolls" (Philippines), and "IOs (information operations)" (Thailand) to circulate manipulative narratives discrediting their political opponents.

Some politicians even fanned the flames of religious (Indonesia/Thailand) and ethnic conflict (all three) in their communities in a desperate bid to score votes.

Meanwhile, tech platforms, journalists, and factcheckers struggle to catch up with disinformation architects' savvy innovations.

Rather than mitigate disinformation, state actors and government legislators across these countries have been found to be directly responsible for producing political disinformation themselves.

This report offers a regional assessment of current practices in election - related social media manipulation and interventions with the aim of mitigating future risks in the global context.

This report synthesizes original research separately conducted by Ong (Thailand) and Tapsell (Indonesia) as well as collaborative research they conducted for an election integrity intervention in the Philippines.

Our research methods are primarily qualitative–drawing from interviews with politicians, campaigners, digital strategists, and journalists–and digital ethnography based on long-term observation of online communities across social media platforms.

This report summarizes trends of electionrelated disinformation production from these three Southeast Asian countries to offer insight and comparison for other countries.

Their high level of digital activity, robust (sometimes underground) digital economies, and complex histories of political polarization possibly preview forthcoming global trends.

To read more:
https://www.stratcomcoe.org/mitigating-disinformation-southeast-asian-elections

	Indonesia	Philippines	Thailand
Key narratives of disinformation	Questioning candidate's Islamic piety anti-communism anti-China extreme speech	populist narrative demonizing "elite" politicians and the press historical revisionism anti-China extreme speech	nationalist discourse targeting anti-monarchy factions hate speech against Malay Muslim minority

Number 5

New technique separates industrial noise from natural seismic signals

A transformative, cloud-computing approach to analyzing data helps researchers better understand seismic activity

Los Alamos National Laboratory
Delivering science and technology to protect our nation and promote world stability

For the first time, seismologists can characterize signals as a result of some industrial human activity on a continent-wide scale using cloud computing.

In two recently published papers in Seismological Research Letters, scientists from Los Alamos National Laboratory demonstrate how previously characterized "noise" can now be viewed as a specific signal in a large geographical area thanks to an innovative approach to seismic data analyses.

"In the past, human-caused seismic signals as a result of industrial activities were viewed as 'noise' that polluted a dataset, resulting in otherwise useful data being dismissed," said Omar Marcillo, a seismologist at Los Alamos National Laboratory and lead author of the study. "For the first time, we were able to identify this noise from some large machines as a distinct signal and pull it from the dataset, allowing us to separate natural signals from anthropogenic ones."

The study used a year's worth of data from more than 1,700 seismic stations in the contiguous United States. Marcillo detected approximately 1.5 million industrial noise sequences, which corresponds on average to around 2.4 detections per day at each station.

"This shows us just how ubiquitous industrial noise is," said Marcillo. "It's important that we're able to characterize it and separate it from the other seismic signals so we can understand exactly what we're looking at when we analyze seismic activity."

This data was accessed and processed using cloud computing—a novel approach that allows for greater scalability and flexibility in seismological research.

The approach is detailed in a companion paper, which demonstrated how cloud computing services can be used to do large-scale seismic analysis ten times faster than traditional computing, which requires data to be downloaded, stored, and processed.

Using Amazon Web Services' cloud computing, researchers were able to acquire and process 5.6 terabytes of compressed seismic data in just 80 hours. To do this using traditional computing methods would have taken several weeks.

Marcillo said that his work to characterize industrial noise across the country would not have been possible without this new cloud-computing approach. "My colleagues and I had figured out how to separate the industrial noise signal from the rest of the seismic signal, but we couldn't scale it," he said. So Marcillo collaborated with Jonathan MacCarthy to find a way to expand it to cover a large geographical area; cloud computing was the answer. It is also flexible enough to adapt to the evolving needs of many research applications, including processing speed, memory requirements, and different processing architectures.

"Seismology is a data-rich field," said MacCarthy, lead author of the paper on the cloud-based approach. "Previously, seismic data would have to be downloaded and processed by each individual researcher. Cloud computing allows all of that data to be stored in one place, and for researchers to easily access and work with it in a community-based way. It's a huge development and has the potential to totally transform the way seismological research on large datasets is done."

To read more:
https://www.lanl.gov/discover/news-release-archive/2020/May/0519-industrial-noise.php?source=newsroom

Number 6

European insurers face increased risk exposures due to Covid-19, but market perceptions and imbalances remained at medium level

The European Insurance and Occupational Pensions Authority (EIOPA) published its updated Risk Dashboard based on the fourth quarter 2019 Solvency II data.

Despite the fact that some indicators used in this Risk Dashboard do not capture the latest market development in the context of Covid-19 outbreak, the expected deterioration of the relevant indicators reflecting all available information in a forward looking perspective has been considered in the assigned risk levels. This addresses the current situation of high uncertainty in the insurance market.

The results show that the risk exposures of the European Union insurance sector increased as the outbreak of Covid-19 strongly affected the lives of all European citizens with disruptions in all financial sectors and economic activities.

Macro and market risks indicators deteriorated in March 2020, moving from high to very high level.

The macroeconomic environment has been affected strongly by the global lockdown.

GDP estimate points to a strong downturn for the first quarter 2020 and latest forecasts predict a recession worldwide for 2020.

Inflation forecasts have been revised downwards for the next four quarters.

Monetary policy support has been activated by all major central banks.

Financial markets have been characterized by sell-off across asset classes, increased volatilities for bond and equity markets, increasing risk premia and flight to quality investment behaviour in March 2020.

Credit risk has increased across all asset classes, in particular CDS of government bonds, financial and non-financial corporate bonds have increased sharply.

Liquidity and funding risks have been raised to high level due to potential additional strains on the disposable liquidity of insurers in the medium to long-term horizon.

For Q4-2019 liquidity indicators were broadly stable, however some are expected to worsen, triggered by possible decrease in premiums and new business, potential increase in claims and illiquid level of certain assets. Profitability and solvency risks have increased to high level.

Although for Q4-2019 insurers solvency positions remained relatively stable, looking ahead profitability and solvency risks are expected to deteriorate, given the double-hit scenario negatively affecting insurers on both asset and liability side. Insurance risks also raised to high level.

While broadly stable in Q4-2019, negative effects via income reduction and increase in claims are expected going forward.

Market perceptions remain at medium level albeit deteriorating. The EU insurance sector underperformed the market, both life and non-life businesses lines, and the median price-to-earnings ratio of insurance groups in the sample decreased since the last assessment.

Insurers' external ratings and rating outlooks do not show sign of deterioration as of end March 2020, however credit quality is expected to deteriorate.

Risks	Level	Trend
1. Macro risks	Very High	↑
2. Credit risks	High	↑
3. Market risks	Very high	↑
4. Liquidity and funding risks	High	↗
5. Profitability and solvency	High	↗
6. Interlinkages and imbalances	Medium	→
7. Insurance (underwriting) risks	High	↗
8. Market perceptions	Medium	↗

Background

This Risk Dashboard based on Solvency II data summarises the main risks and vulnerabilities in the European Union insurance sector through a set of risk indicators of the fourth quarter of 2019 complemented with market data and other available information.

This data is based on financial stability and prudential reporting collected from 96 insurance groups and 2837 solo insurance undertakings.

To read more:
https://www.eiopa.europa.eu/risk-dashboard

https://www.eiopa.europa.eu/sites/default/files/financial_stability/risk_dashboard/eiopa-bos-20-274-april-2020-risk-dashboard.pdf

Macro risks[2]	↑
	Level: very high
	Trend: increase
Macro risks increased from high to very high given the global impact of the outbreak of COVID on economic activities. GDP growth forecasts have been revised significantly downwards for all geographical areas, while inflation is expected to decrease slightly. The indicator on the 10 year swap rates decreased reaching new lows, after a flattening of all swap curves on the long end. Unemployment rate is expected to increase, due to steep fall of business activities fiscal balances are expected to deteriorate as government announced their interventions to sustain the halted economies. Monetary support has been activated by all major central banks.	

Number 7

Actions Needed to Enhance DHS Oversight of Cybersecurity at High-Risk Chemical Facilities

United States Government Accountability Office

GAO

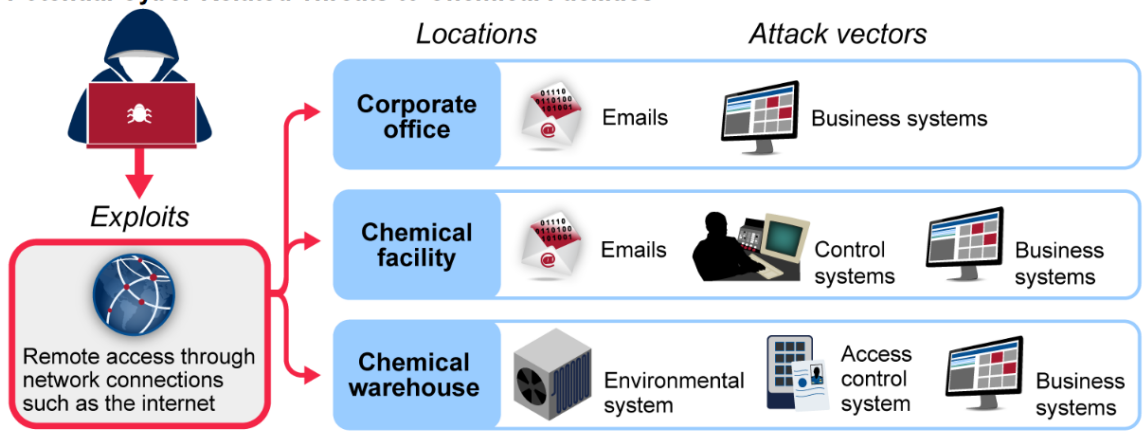
Report to Congressional Requesters

The Chemical Facility Anti-Terrorism Standards (CFATS) program within the Department of Homeland Security (DHS) evaluates high-risk chemical facilities' cybersecurity efforts via inspections that include reviewing policies and procedures, interviewing relevant officials, and verifying facilities' implementation of agreed-upon security measures.

GAO found that the CFATS program hasguidance designed to help the estimated 3,300 CFATS-covered facilities comply with cybersecurity and other standards, but the guidance has not been updated in more than 10 years, in contrast with internal control standards which recommend periodic review.

CFATS officials stated that the program does not have a process to routinely review its cybersecurity guidance to ensure that it is up to date with current threats and technological advances. Without such a process, facilities could be more vulnerable to cyber-related threats.

Potential Cyber-Related Threats to Chemical Facilities



Source: GAO analysis of potential cybersecurity threats to chemical facilities. | GAO-20-453

The CFATS program developed and provided cybersecurity training for its inspectors, but GAO found that the CFATS program does not fully address 3 of 4 key training practices, or address cybersecurity needs in its workforce planning process, as recommended by DHS guidance.

Specifically:

• The CFATS program does not:

(1) systematically collect or track data related to inspectors' cybersecurity training or knowledge, skills, and abilities;

(2) develop measures to assess how training is contributing to cybersecurity-related program results; or

(3) have a process to evaluate the effectiveness of its cybersecurity training in improving inspector skillsets.

• The program also has yet to incorporate identified cybersecurity knowledge, skills, and abilities for inspectors in its current workforce planning processes or track data related to covered facilities' reliance on information systems when assessing its workforce needs.

Fully addressing key training practices will help ensure that CFATS inspectors have the knowledge, skills, and abilities for cybersecurity inspections, and identifying cybersecurity needs in workforce planning will help the program ensure that it has the appropriate number of staff to carry out the program's cybersecurity-related efforts.

To read more:
https://www.gao.gov/assets/710/706972.pdf

Number 8

Data and Technology Research Project Update Spotlight

PCAOB
Public Company Accounting Oversight Board

Advancements in technology are affecting the nature, timing, preparation, and use of financial information.

Some audit firms are making significant investments in personnel and other resources to expand their use of technology-based audit tools, including software used to perform data analytics (technology-based tools), to plan and perform audits.

In light of the increasing use of technology by auditors and preparers, the Board's strategic plan highlights that we must anticipate and respond to these innovations and their corresponding opportunities and risks.

The PCAOB's Office of the Chief Auditor established a research project on data and technology to assess whether there is a need for guidance, changes to PCAOB standards, or other regulatory actions.

As part of assessing whether regulatory action is necessary in response to the evolving audit landscape, we have gathered information from PCAOB oversight activities, reviewed changes to firms' methodologies, and studied relevant academic research.

We have engaged with key stakeholders on their experiences with data and technology and have monitored the activities of other standard setters and regulators.

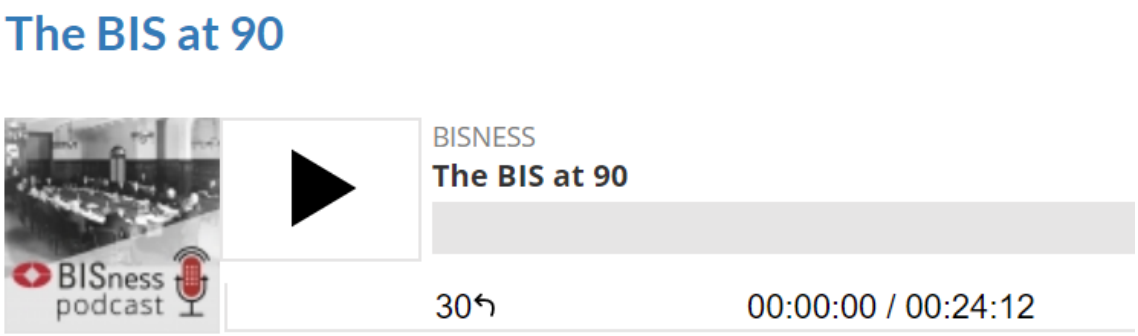
Our work has also been informed by the PCAOB Data and Technology Task Force (Task Force), whose members provide additional insights into the use of technology by auditors and preparers.

This Spotlight shares certain observations from our research and outreach activities. To read more:
https://pcaobus.org/Documents/Data-Technology-Project-Spotlight.pdf

Number 9

The BIS at 90

Piet Clement explains the origins of the BIS and the roles it has played since opening on 17 May 1930.



The BIS was created in 1930 by the Hague Conference as an international financial organisation. Ever since, its key mandate has been to foster cooperation among central banks and other agencies in pursuit of monetary and financial stability.

Initially mainly focused on Europe, the BIS, from the 1960s onward, became increasingly global in its activities and outreach. Today it brings together sixty member central banks, representing countries from around the world that together make up about 95% of world GDP.

Apart from its headquarters in Basel, Switzerland, the BIS has two representative offices, one for Asia and the Pacific in Hong Kong SAR (since 1998), and one for the Americas in Mexico City (since 2002).

Throughout its history, the BIS has been involved in many historical events and developments in the monetary and financial sphere. These include the repercussions of the world financial crisis of 1931, the rebuilding of European multilateral payments in the 1950s, the transatlantic management of the Bretton Woods system in the 1960s, and the international efforts to deal with the fall-out of inflation and of the banking and debt crises in the 1970s through the 1990s.

The BIS played an important role in the early history of European monetary unification (before the foundation of the European Monetary Institute in Frankfurt in 1994). It also hosts the experts from the global banking regulation and supervision community, who have been responsible for developing an International Capital Framework (known consecutively as

Basel Accord, Basel II and Basel III), a global agreement aimed at strengthening capital adequacy rules for internationally active banks.

You may visit:
https://bispodcast.libsyn.com/the-bis-at-90

Number 10

Notice of cyber security incident

easyJet plc

Following discussions with the Information Commissioner's Office ("ICO"), the Board of easyJet announces that it has been the target of an attack from a highly sophisticated source.

As soon as we became aware of the attack, we took immediate steps to respond to and manage the incident and engaged leading forensic experts to investigate the issue. We also notified the National Cyber Security Centre and the ICO. We have closed off this unauthorised access.

Our investigation found that the email address and travel details of approximately 9 million customers were accessed. These affected customers will be contacted in the next few days. If you are not contacted then your information has not been accessed. Other than as referenced in the following paragraph, passport details and credit card details of these customers were not accessed.

Our forensic investigation found that, for a very small subset of customers (2,208), credit card details were accessed. Action has already been taken to contact all of these customers and they have been offered support.

We take issues of security extremely seriously and continue to invest to further enhance our security environment.

There is no evidence that any personal information of any nature has been misused, however, on the recommendation of the ICO, we are communicating with the approximately 9 million customers whose travel details were accessed to advise them of protective steps to minimise any risk of potential phishing.

We are advising customers to continue to be alert as they would normally be, especially should they receive any unsolicited communications. We also advise customers to be cautious of any communications purporting to come from easyJet or easyJet Holidays.

We're sorry that this has happened, and we would like to reassure customers that we take the safety and security of their information very seriously. To read more: http://otp.investis.com/clients/uk/easyjet1/rns/regulatory-story.aspx?cid=2&newsid=1391756

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.

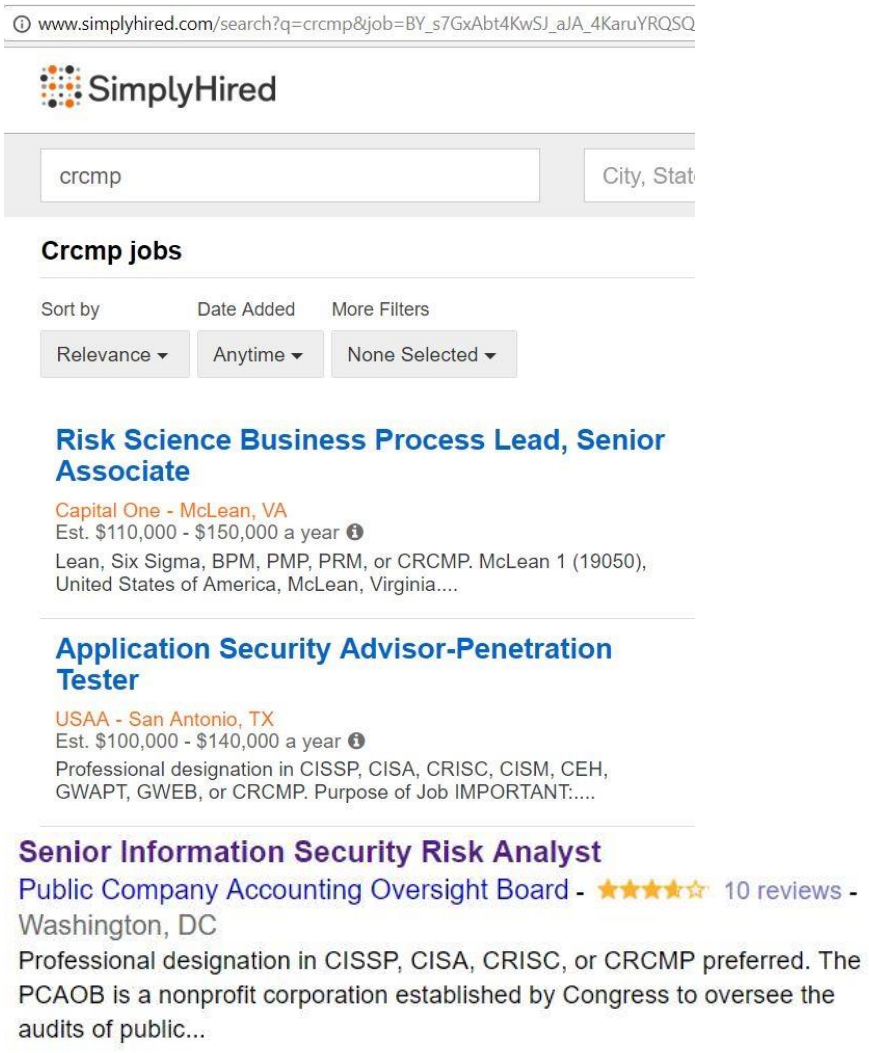
International Association of Risk and Compliance Professionals

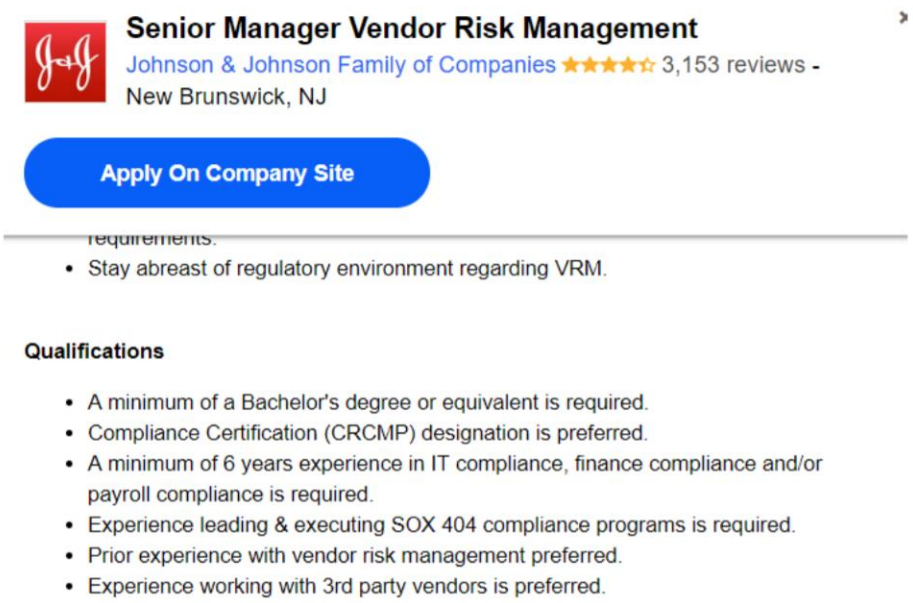
You can explore what we offer to our members:

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