International Association of Risk and Compliance Professionals (IARCP)
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA
Tel: 202-449-9750, Web: www.risk-compliance-association.com

Monday, July 19, 2021

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

Dear members and friends,

How could the global economy evolve from here? What could "pandexit" look like?

Who asks questions like that? The new Annual Economic Report from the Bank for International Settlements (BIS).

How can we answer questions like that? We cannot, but we have to do our best, using financial stress testing. Of course, we will use adverse scenarios that are "severe yet plausible" (severe enough to be meaningful, yet plausible enough to be taken seriously). We will follow Ovid's advice: *Perfer et obdura, dolor hic tibi proderit olim* - be patient and tough; someday this pain will be useful to you.

We read in the BIS Annual Economic Report that given the uncertainties involved, and before turning to policy, it is worth considering *three*

plausible scenarios: the *central one* embodied in current consensus forecasts, *one* in which inflation proves stronger than expected and financial market conditions tighten, and *one* in which the global recovery falters and the economy fails to recover.

Of course, various combinations are also possible. The future will not be so tidy, and individual countries will experience different permutations. Even so, together the scenarios provide a useful range of plausible outcomes that helps clarify the challenges policymakers face.

Which are the three scenarios?

The *central scenario* sees a comparatively smooth recovery. The pandemic is steadily brought under control. Consumption sustains the expansion. Corporate sector losses remain limited, and sectoral reallocation proceeds smoothly.

In the main jurisdictions, inflation rises towards targets and any increase beyond them is temporary. Financial conditions do not tighten significantly. Even in this scenario, however, significant cross-country differences remain. The world entered the crisis suddenly and as one; countries will "pandexit" at their own speed and in their own way. In particular, growth in many EMEs lags behind, even as some see more persistent inflation.

The *second scenario* is one where, on the back of stronger growth, inflation exceeds expectations and financial conditions tighten. Markets anticipate a quicker and possibly more intense monetary policy tightening. This is consistent with a larger impact of fiscal policy on demand and a bigger reversal in saving rates than assumed in the central scenario, possibly supported by better news on the pandemic front.

How plausible is this scenario? To be sure, the longer-term forces holding inflation down are still with us, notably globalisation and technological advances: these have weakened the pricing power of both labour and firms.

Moreover, the responsiveness of inflation to pressures on productive capacity has been extremely low for well over a decade now. That said, non-linearities cannot be ruled out. And even if any increase in inflation ultimately proves temporary, financial market participants could overreact, anticipating more sustained inflation.

Either way, the tightening could be substantial, as participants could be caught wrong-footed and be forced to unwind their positions. The

prolonged aggressive risk-taking that has prevailed in markets for so long increases the probability of such an outcome.

Recent localised stress, such as the Archegos failure and the losses it has inflicted on banks, could turn out to be the proverbial canary in the coalmine. A key question concerns the resilience of non-bank financial intermediation, especially in the context of hidden leverage and liquidity mismatches.

The *third scenario*, in which the recovery stalls, is more plausible if the pandemic proves harder to control. Successive waves of more virulent Covid strains could be impervious to vaccines, leading to tighter containment measures.

Fiscal multipliers and the deployment of excess savings could fall short of expectations. In particular, the feared wave of firms' insolvencies could materialise – another big question mark clouding the outlook. Estimates of likely credit losses embodied in the central scenario suggest that they would be manageable. Importantly, the debt in the most affected sectors accounts for a relatively small fraction of the total.

But this conclusion hinges on policy support being there for as long as necessary. In this alternative scenario, firms' losses could be larger, possibly on a par with those during the Great Financial Crisis (GFC). In turn, banks could feel the strain. In fact, some of them have taken back part of the provisions made earlier in 2020, indicating that they could be caught by surprise.

Read more at Number 1 below. Welcome to the Top 10 list.

Best regards,

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

Number 1 (Page 6)

BIS Annual Economic Report

Number 2 (Page 8)

Investor Alerts and Bulletins

Funds Trading in Bitcoin Futures

Number 3 (Page 11)

Climate, ESG, and the Board of Directors: "You Cannot Direct the Wind, But You Can Adjust Your Sails"

Commissioner Allison Herren Lee, SEC, Keynote Address at the 2021 Society for Corporate Governance National Conference, Washington D.C.

Number 4 (Page 14)

Joint ECB/ESRB report shows uneven impacts of climate change for the EU financial sector

Number 5 (Page 17)

Climate stress testing – a new kid on the block

Climate-related risk and financial stability - ECB/ESRB Project Team on climate risk monitoring

Number 6 (Page 20)

Thirty years of hurt, never stopped me dreaming

Andrew G Haldane, Executive Director and Chief Economist of the Bank of England, at the Institute for Government.

Number 7 (Page 25)

Phishing most common Cyber Incident faced by SMEs

The European Union Agency for Cybersecurity identifies the cybersecurity challenges SMEs face today and issues recommendations.

Number 8 (Page 28)

Data of 700 million LinkedIn users reportedly advertised on dark web

Number 9 (Page 30)

Thousands of fake online pharmacies shut down in INTERPOL operation

Number 10 (Page 33)

Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments

Number 1

BIS Annual Economic Report

BIS

Introduction

It is now over a year since the Covid-19 pandemic struck out of the blue, plunging the global economy into a historically deep recession.

An acute health crisis turned into an overwhelming economic crisis, as policymakers adopted stringent containment measures to save lives.

This was a recession in response to an insidious invisible enemy.

A timely, forceful and concerted policy drive prevented the worst. Working together, monetary, fiscal and prudential authorities managed to stabilise the financial system and cushion the blow. They put the patient in a state of suspended animation.

But as last year's Annual Economic Report (AER) went to press, uncertainty still reigned: what would happen next? There was hardly any precedent to serve as a benchmark. No recent pandemic was remotely as damaging as the current one.

And the Spanish flu outbreak was too distant and too different. Many central banks suspended publishing forecasts, turning to tentative scenarios instead.

Where do we stand today? We know much more about the enemy and we are better equipped to fight it. We know much more about how the economy responds and how far it can adjust.

The patient is in much better health but has not yet fully recovered. Some parts of the body are in better shape than others. What is clear is that the recovery will be uneven and the long-term consequences material.

"Pandexit" will be bumpy and leave a costly and long-lasting legacy.

How has the global economy fared during the past year? What are the prospects and risks? What are the policy challenges?

While central banks were tackling the consequences of the pandemic, other important issues continued to draw attention.

Questions pertaining to the relationship between monetary policy and inequality moved to the centre of public discourse.

In addition, discussion and analysis of central bank digital currencies (CBDCs) became livelier than ever.

What follows elaborates on these issues.

A surprisingly strong but very uneven recovery

Starting in the second half of 2020, the global economy rebounded more strongly than anticipated.

Private consumption was the main engine of growth.

As Covid-19 broke out, there had been widespread concerns about "scarring effects" on consumers' spending.

It had been feared that lingering risk aversion and contagion worries would hold it back. In the event, these fears proved unfounded.

The craving for normality prevailed.

Whenever containment measures were relaxed in contactintensive services, demand returned swiftly.

In addition, as consumers adapted, a further shift to e-commerce limited the restrictions' fallout.

At the same time, rates of change should not be confused with levels. For the year as a whole, GDP still declined by some 3.4%.

To be sure, at the time of writing world GDP has more or less returned to its pre-crisis level. But this masks a clear divide between China, where GDP is now well above its pre-crisis level, and the rest of the world, where it is still generally some way below.

To read more: https://www.bis.org/publ/arpdf/ar2021e.pdf

Number 2

Investor Alerts and Bulletins

Funds Trading in Bitcoin Futures

U.S. SECURITIES AND EXCHANGE COMMISSION

The Securities and Exchange Commission's (SEC's) Office of Investor Education and Advocacy (OIEA) and the Commodity Futures Trading Commission's (CFTC's) Office of Customer Education and Outreach (OCEO) urge investors considering a fund with exposure to the Bitcoin futures market to weigh carefully the potential risks and benefits of the investment.

Among other things, investors should understand that Bitcoin, including gaining exposure through the Bitcoin futures market, is a highly speculative investment.

As such, investors should consider the volatility of Bitcoin and the Bitcoin futures market, as well as the lack of regulation and potential for fraud or manipulation in the underlying Bitcoin market.

Bitcoin. Bitcoin is a digital asset, or an asset that relies on blockchain technology. Bitcoin has also been called a "virtual currency" or a "cryptocurrency."

Bitcoin future. A Bitcoin futures contract is a standardized agreement to buy or sell a specific quantity of Bitcoin at a specified price on a particular date in the future. In the United States, Bitcoin is a commodity, and commodity futures trading is required to take place on futures exchanges regulated and supervised by the CFTC.

Funds regulated under the Investment Company Act of 1940 and its rules ("funds") are required to provide important investor protections.

For example, funds must comply with legal requirements related to valuation and custody of fund assets, and mutual funds and ETFs must comply with liquidity requirements.

Those protections apply to all of a fund's holdings, including holdings of Bitcoin futures contracts.

Some funds may engage in the trading of Bitcoin futures contracts as one way to gain exposure to Bitcoin. Investors should understand that positions in Bitcoin and Bitcoin futures contracts are highly speculative.

Investors who are thinking about investing in a fund that buys or sells Bitcoin futures should carefully consider:

- *The investor's risk tolerance*. Investors should focus on the level of risk they are taking compared to the level of risk they are comfortable taking. For more information, read Assessing Your Risk Tolerance.

- *The fund's disclosure of its risks*. A fund is required to disclose the principal risks of investing in the fund in its prospectus. For more information read, How to Read a Mutual Fund Prospectus (Part 1 of 3: Investment Objective, Strategies, and Risks).

- *Potential loss of the investment*. All investments in funds involve risk of financial loss. This risk may be increased for positions in Bitcoin futures contracts because of the high volatility of Bitcoin and Bitcoin futures (meaning prices can fluctuate widely). There is also the potential for fraud and manipulation in the underlying cash or "spot" Bitcoin market.

- *Difference in investment outcome*. A rise in Bitcoin prices may not result in a similar increase in the value of a fund holding positions in Bitcoin futures contracts.

  This is in part because funds that trade commodity futures contracts may not have direct exposure to the contracts' underlying assets.

  Futures contract prices can vary by delivery months and differ from the underlying commodity's spot price.

  Futures contracts also expire periodically, resulting in fluctuations of portfolio exposure as expiring futures positions are typically rolled into new contracts.

  The value of a particular fund may be affected by this maintenance of futures contract exposure.

  For more information about funds or exchange traded products that trade commodity futures, see Learn About Risks Before Investing in Commodity ETPs or Funds. You may visit: https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/CustomerAdvisory_CommodityETPs.htm

Funds that buy or sell Bitcoin futures may have unique characteristics and heightened risks compared to other funds. It is important to consider how any investment fits into your overall investment plan before investing.

Note: This Investor Bulletin represents the views of the staff of the SEC's Office of Investor Education and Advocacy and CFTC's Office of Customer Education and Outreach. It is not a rule, regulation, or statement of the Securities and Exchange Commission or the Commodity Futures Trading Commission (the "Commissions"). The Commissions have neither approved nor disapproved its content. This Bulletin, like all staff statements, has no legal force or effect: it does not alter or amend applicable law, and it does not create any enforceable rights or new or additional obligations for any person.

Number 3

Climate, ESG, and the Board of Directors: "You Cannot Direct the Wind, But You Can Adjust Your Sails"

Commissioner Allison Herren Lee, SEC, Keynote Address at the 2021 Society for Corporate Governance National Conference, Washington D.C.

Good morning and thank you for the invitation to speak today at the Society for Corporate Governance 2021 National Conference. I'm impressed with your full and informative agenda over the next few days, and I appreciate the important work you do in supporting company boards and executives.

I also appreciate your engagement in the SEC's policymaking process, including your recent letter in response to the request for public input on climate change disclosures.

In fact, we've received thousands of comments in response to that request, but we hardly need that statistic to understand that the subject of climate risk and our financial markets, and ESG more broadly, is top of mind in board rooms and c-suites around the globe.

Increasingly, boards of directors are called upon to navigate the challenges presented by climate change, racial injustice, economic inequality, and numerous other issues that are fundamental to the success and sustainability of companies, financial markets, and our economy.

This call, welcomed by some and eschewed by others, is attributable in part to the large and growing influence that corporations hold over the social and economic well-being of people and communities everywhere.

A study from 2018, for example, showed that 71 of the top 100 revenue generators globally were corporations while only 29 were countries.

In other words, corporations – in many cases U.S. corporations – often operate on a level or higher economic footing than some of the largest governments in the world.

That is a dynamic worthy of reflection – and one that drives home the weighty consequences and obligations associated with some corporate decisions.

Small wonder, then, that not just investors, but employees, consumers, vendors, suppliers, and numerous other stakeholders, look to companies to design and implement long-term, sustainable policies that support growth and address the environmental and social impacts these companies have. And these expectations increasingly play out in ways that were far less a part of the corporate consciousness just a decade or two ago.

Today, what your business does and says is as likely to be dissected on Twitter and TikTok as it is to be reported in the Wall Street Journal or over a newswire.

Consequently, consumers, employees, both current and potential, and a host of others can affect how companies are perceived and how well they succeed.

I know many in this virtual room, including those on boards of directors, understand this dynamic. And understand that these environmental and social issues, once perhaps treated as more peripheral, are now central business considerations.

So boards are stepping up their engagement on climate and ESG related-risks and opportunities. For instance, in one recent survey, nearly 80 percent of directors reported that their boards are focused on some aspect of ESG.

An analysis of a selection of S&P 100 proxy statements found that 78 percent of companies had at least one board committee charged with overseeing environmental sustainability matters.

And 42 percent of companies reviewed in that analysis associated at least one director with expertise in environmental policy, sustainability, corporate responsibility, or ESG.

At the same time, while many companies report that they oversee ESG at the board level, some analysis suggests they may lack specific sustainability mandates and do not demonstrate board-management engagement on ESG.

In addition, there are some indicators that reported board expertise on ESG may be ill-defined and still lacking. There is more work to be done.

Because, in the words of prominent corporate attorney Marty Lipton, “a corporation ignores environmental and social challenges at its own peril.”

To read more:
https://www.sec.gov/news/speech/lee-climate-esg-board-of-directors

Number 4

Joint ECB/ESRB report shows uneven impacts of climate change for the EU financial sector

EUROPEAN CENTRAL BANK
EUROSYSTEM

- Financial stability vulnerabilities from climate change concentrated in certain regions, sectors and firms, with evolution of risks conditional on effective and timely transition to low carbon economy

- Granular exposure mapping of climate hazards to financial risk reveals vulnerability to river flooding widespread across countries, compounded by wildfire, heat and water stress risk in some regions

- Transition risk resulting from financial market repricing has cross-sector impact and varies within sectors owing to differences in emissions efficiency

- Long-term scenario analyses suggest timely and orderly macroeconomic policies to tackle climate-related risk can reduce financial stability risks, notably for highest greenhouse-gas emitting sectors

The European Central Bank (ECB) and the European Systemic Risk Board (ESRB) published a joint report that takes a closer look at how a broadened set of climate change drivers affects millions of global firms and thousands of financial firms in the European Union (EU). It maps out prospective financial stability risks and contributes by further developing the analytical basis for more targeted and effective policy action. The report: https://www.ecb.europa.eu/pub/pdf/other/ecb.climateriskfinancialstability202107~87822fae81.en.pdf

Climate-related risk and financial stability

ECB/ESRB Project Team on climate risk monitoring

The report tackles measurement gaps and, building on previous work in this field, establishes a detailed topology of physical and transition risks arising from climate change across regions, sectors and firms. It also applies a scenario analysis with long-dated financial risk horizons to capture prospective financial losses resulting from the timeliness and effectiveness of climate policies and technologies.

"These findings underline the crucial and urgent need for climate policies and economic transitions, not only to ensure that the targets of the Paris Agreement are met, but also to limit the long-run disruption to our economies, businesses and livelihoods," said Christine Lagarde, President of the ECB and ESRB Chair.

The report's granular mapping of financial exposures to climate change drivers finds three forms of risk concentration.

First, exposures to physical climate hazards are concentrated at the regional level. The analysis shows, for example, that river floods will be the most economically significant widespread climate risk driver in the EU over the next two decades compounded by strong vulnerability to wildfires, heat and water stress in some regions.

Around 30% of the euro area banking sector's credit exposures to non-financial companies are to firms that are subject to a combination of these physical hazards.

Second, exposures to emission-intensive firms are concentrated not only across but also within economic sectors.

Exposures to highly emitting firms occupy 14% of collective euro area banking sector balance sheets. While mainly concentrated in the manufacturing, electricity, transportation and construction sectors, they also vary considerably within sectors – suggesting scope for financial market repricing as widely varying emissions intensities narrow.

Third, exposures to climate risk drivers are concentrated in specific European financial intermediaries.

Around 70% of banking system credit exposures to firms subject to high or increasing physical risk over the coming decades are concentrated in the portfolios of just 25 banks.

At the same time, scope for financial market repricing associated with transition risk will be particularly large for investment funds, where more than 55% of investments are tilted toward high emitting firms and

estimated alignment with the EU Taxonomy stands at only 1% of assets. While direct holdings by insurers of climate sensitive assets may be manageable, risks could be amplified by cross-holdings of investment funds of around 30%.

Long-term scenario analysis for EU banks, insurers and investment funds suggests that credit and market risk could increase as a result of a failure to effectively counteract global warming.

In the projected scenario modelling what would happen in the event of an insufficiently orderly climate transition, physical risk losses – particularly for high emitting firms – would become dominant in around 15 years. This could lead to a decline in global GDP of up to 20% by the end of the century should mitigation prove to be insufficient or ineffective.

As work continues on more accurately measuring and modelling climate risk, the advances described in this report should provide valuable evidence to inform the broadening climate debate in the public and private sector alike.

Number 5

Climate stress testing – a new kid on the block

Climate-related risk and financial stability - ECB/ESRB Project Team on climate risk monitoring

In recent years progress has been made on climate stress testing and scenario analysis methodologies. This has been possible thanks to growing experience and the increased availability of datasets.

The following three sections discuss the challenges of climate-related scenario analysis for the financial sector.

The first two discuss trends in the area of forward-looking scenario analysis, while the third and the last section of the report puts these methodologies into use in a coordinated climate-sensitivity analysis of the European financial sector.

The Handbook in Annex 2 “Detailed look at existing methodologies” provides a complete overview of off-the-shelf methodologies developed in European institutions.

The Handbook is designed as a practical guide for practitioners and aims to foster the development of climate-related methodologies in other institutions.

It describes in detail different approaches to estimate key parameters that connect the non-financial sector, which could be impacted by climate-related shocks, and the financial sector’s balance sheets.

Since the publication of the first report of the ECB/ESRB Project Team on climate risk monitoring, central banks and supervisors have intensified their efforts to develop climate-related stress testing frameworks.

International organisations have also joined the call to incorporate climate-related risks in stress-testing exercises, including the International Monetary Fund (IMF) (2020a, 2020b), the Bank for International Settlements (BIS) (2020), the Financial Stability Board (FSB) (2020, 2021), and the Network for Greening the Financial System (NGFS) (2021).

European Union authorities have completed or are in the process of conducting or planning 18 climate stress test exercises.

The climate-related scenario analysis is gradually shifting towards stressing both physical and transition risks. As shown in Chart 16 (left panel), all of the stress testing and sensitivity initiatives completed up to 2020 focus on transition risks. However, from 2021 there is a growing number of exercises covering physical and transition risks.

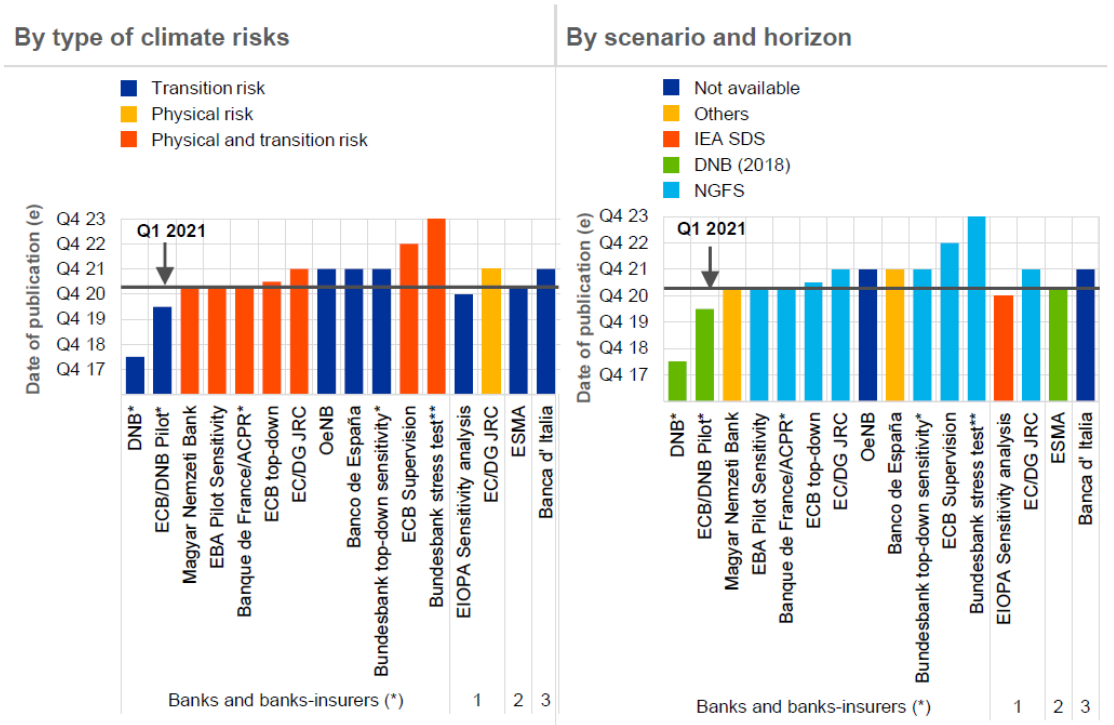
This trend is coupled with an extension of the horizon used in scenario analysis (Chart 16, right panel). The initial transition risk-focused stress test exercises relied on scenarios with a five-year horizon.

This was an extension compared with the more standard three-year horizon used in regular stress test exercises, but far shorter than the horizon of up to the year 2100 included in NGFS scenarios.

The ongoing exercises are bolder, extending to a 30-year horizon in most cases. The NGFS scenarios are becoming a common reference for ongoing and planned exercises, in particular, the orderly transition, the disorderly transition (with two variants, namely with effective and ineffective transition policies) and the "hot house world" scenario discussed in Section 6.

Chart 16

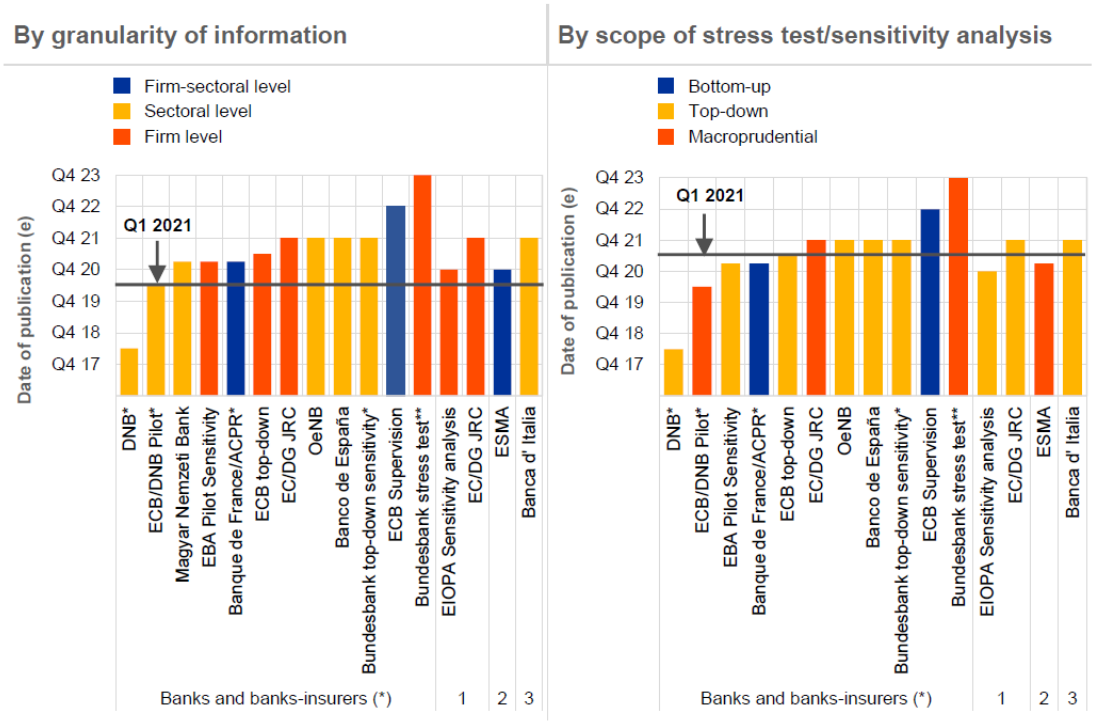
Initiatives of climate-related stress test and sensitivity analysis in European Union institutions



Climate-related stress-testing and sensitivity frameworks have evolved towards the use of increasingly granular data. As shown in Chart 17 (left panel), early exercises employed mostly sector-level information, e.g. sector-level CO2 intensity.

Chart 17

Initiatives of climate-related stress test and sensitivity analysis in European Union institutions



It reflected the fact that disclosure of climate-related risks from private entities has been insufficient, heterogeneous and patchy.

As databases of climate risk and exposure information have been gradually improving and are made available, several institutions have started or are planning stress-testing exercises extensively using firm-level information or, in some cases, transaction-level information.

To read more (at page 51/111) you may visit:
https://www.ecb.europa.eu/pub/pdf/other/ecb.climateriskfinancialstability202107~87822fae81.en.pdf

Number 6

Thirty years of hurt, never stopped me dreaming

Andrew G Haldane, Executive Director and Chief Economist of the Bank of England, at the Institute for Government.

At the end of September I leave the Bank of England, 32 years almost to the day since I joined. Most would say that is a decent stint, but in Bank terms it is just really getting started.

My personal assistant, the brilliant Sandra Mills, has just completed 44 years. The Bank's company secretary, John Footman, is just about to clock 52 years. I never was a completer-finisher.
It has not, of course, been 30 years of hurt.

I have loved almost all of my time at the Bank. I promised myself one thing when I joined - that I would only stay as long as it was interesting. It has been interesting for 32 years. Events made it so. And it remains no less interesting now.

I tell the Bank's new entrants I can promise them only one thing: they will be telling their families and friends about this moment in history and, uniquely, they can write its next chapter. As a public servant, this is as good as it gets.

Any lengthy career in public policy will inevitably be punctuated by crisis. In my case, crises have provided not just the punctuation marks, but most of the words, sentences and paragraphs too. In public policy, crises are the ultimate learning experience.

They are also the moments when the Overton window of opportunity is widest and the opportunity for change greatest. Crises are moments of challenge and opportunity in equal measure. I am very fortunate to have experienced plenty of both.

My time of the Bank has been evenly split between its twin statutory functions, monetary and financial stability. These functions, embedded in the Bank's Royal Charter in 1694, remain its statutory centrepiece

today. (The Bank's third objective, fighting the French, has by contrast tended to be downplayed.) Over the intervening 327 years, both monetary and financial stability have had their fair share of challenges and opportunities. These have perhaps come thicker and faster over the past 27 years than the preceding 300.

I want to offer a few retrospective thoughts on the evolution of monetary and financial stability over the past 30 years before turning to central bank communications, a crucial ingredient of both.

Bank of England policy frameworks and practices have undergone an astonishing transformation over that period. I do not think it is an exaggeration to say there has been a revolution in how the Bank goes about securing monetary and financial stability and how it communicates about both. The catalyst for this revolution has been crisis.

Having discussed this historical evolution-cum-revolution, I discuss some of the key issues facing central banks today. This is the "dreaming" bit - looking around corners to judge not only what is coming but how to reshape it, seeking out the biggest issues not just of today but tomorrow.

It is the Wayne Gretsky approach to public policy - skating to where the puck is going, not where it is.

That can be unconventional and sometimes misunderstood. But it is, for me, the essence of effective policymaking. Imagining a different future is not sufficient for policy success. It is the imagined made real that matters. The Bank is blessed with having the capacity to both think and do, both brain and hands.

When former Governor Cobbold said "the Bank is a bank and not a study group" he was wrong. The Bank is both. And the magic happens when the two are combined, the brains and hands co-ordinated. Nothing illustrates this better than the revolution in the UK's monetary and financial stability frameworks during my tenure.

Monetary policy

I joined the Economics Division of the Bank in 1989, following the well-trodden path from Sunderland council estate to Threadneedle Street. I hoped to redesign the UK's monetary policy framework. My first task fell a fraction short of those ambitions.

It was to forecast the non-resident ("externals") component of the asset

counterparts to M4 (a measure of the money supply). Like the Schleswig-Holstein problem, only three people understood the external counterparts to M4.

One was dead, the other mad and the third was not me. The external counterparts of M4 are as close to a random walk as any time-series on the planet. That makes forecasting them a mug's game. I was that mug. Almost as thankless was the six-monthly forecasting exercise we undertook at the time.

This involved every economist forecasting a component of the National Accounts in microscopic detail. My job was to forecast the Interest, Profits and Dividends component of the UK current account, another lofty task, another random walk, another game of mugs.

At the end of this exhaustive process, the forecasts were sent around the Bank, as well as to HM Treasury. There, I have it on good authority, they quickly became landfill (as recycling wasn't an option at the time).

Like the UK's entry at Eurovision, the Bank economists' contribution was spirited but ultimately pointless. The Bank's analytical brain did not connect to any hands. John Kenneth Galbraith said that economics was extremely useful as a form of employment for economists. At the time, that was the Bank's view too.

The Bank's forecasting process was a fitting metaphor for the UK's monetary policy experience at that point. From the early 1970s onwards, many monetary policy frameworks had been tried. All of them had ended up in the wheelie bin.

In the late 1980s, the UK had no clearly defined nominal anchor for monetary policy at all. The best predictor of interest rate movements was not GDP or inflation. It was whether Mrs Thatcher (the then-Prime Minister) had recently suffered a bad by-election result. Policy played second fiddle to politics.

At the point I joined, the search for another new nominal anchor for the UK was well underway. One of my early tasks was to become an expert on the European Exchange Rate Mechanism (ERM), a framework that was seen as offering a route to monetary redemption for the UK, effectively by outsourcing monetary policy to Germany's Bundesbank.

Within a year, the UK had joined the ERM. And two years later - Black Wednesday, 16 September 1992 - it was forcibly, and ingloriously, ejected.

That day is etched on my memory. I had the incredible good fortune to be sitting on the Bank's foreign exchange dealing desk that day, watching agog as we lost around £20 billion in foreign exchange reserves defending the pound – at the time, real money – despite announcing interest rate rises of 5 percentage points in a single day.

How the world has changed. Currently, financial markets expect UK interest rates to rise by an average 5 basis points each six months for the next 10 years.

The UK's exit from the ERM led to a new nominal anchor being needed. And almost immediately, one was adopted – an inflation target.

It had one obvious merit: it was the only monetary framework not to have already been tried in the UK. But the track record of inflation-targeting was close to non-existent.

At the point the new target was announced, expectations for UK inflation were high (over 5%) and expectations for the framework lasting were low.

The collapse in sterling following sterling's ERM exit, and the expected sharp rise in inflation, meant the wheelie bin beckoned for inflation-targeting.

In the event, inflation failed to pick up as much as expected after the ERM debacle. And, behind the scenes at the Bank, the machinery of monetary policy was changing.

Data, analysis and models suddenly became more central to judgements on inflation and the appropriate monetary stance. Accompanying this, economics and economists began playing a more central role in formulating the Bank's judgements.

Although decisions on interest rates still resided with politicians, the Bank now had a better-informed voice.

That voice became louder as a result of two great leaps forward in monetary policy transparency: the publication by the Bank, from 1993 onwards, of a quarterly Inflation Report; and the publication of monthly minutes of the meetings between the Chancellor and Governor at which monetary policy was decided – the "Ken and Eddie Show".

Both put the Bank's analysis and judgements on the economy and monetary policy in the public domain, for the first time ever.

This did not give the Bank a vote on monetary policy, but did give it a public voice. That voice became increasingly influential in shaping external debate on policy through the 1990s, constraining somewhat the Chancellor's hand.

It also re-shaped the Bank's own processes, which became more rigorous and resource-intensive.

Transparency plus a clear target imposed discipline on the Bank as well as the Chancellor. Whereas before Bank forecasts went into the bin, now they went into the quarterly Inflation Report.

To read more:
https://www.bis.org/review/r210702d.pdf

Number 7

Phishing most common Cyber Incident faced by SMEs

The European Union Agency for Cybersecurity identifies the cybersecurity challenges SMEs face today and issues recommendations.

Small and medium-sized enterprises (SMEs) are considered to be the backbone of Europe's economy. 25 millions of SMEs are active today in the European Union and employ more than 100 million workers.

The report Cybersecurity for SMEs ENISA issues today provides advice for SMEs to successfully cope with cybersecurity challenges, particularly those resulting from the COVID-19 pandemic.

With the current crisis, traditional businesses had to resort to technologies such as QR codes or contactless payments they had never used before.

Although SMEs have turned to such new technologies to maintain their business, they often failed to increase their security in relation to these new systems.
Research and real-life experience show that well prepared organisations deal with cyber incidents in a much more efficient way than those failing to plan or lacking the capabilities they need to address cyber threats correctly.

Juhan Lepassaar, EU Agency for Cybersecurity Executive Director said: "SMEs cybersecurity and support is at the forefront of the EU's cybersecurity strategy for the digital decade and the Agency is fully dedicated to support the SME community in improving their resilience to successfully transform digitally."

In addition to the report, ENISA also publishes today the Cybersecurity Guide for SMEs: "12 steps to securing your business". The short cybersecurity guide provides SMEs with practical high-level actions to better secure their systems, hence their businesses.

Based on an extended desktop research, an extensive survey and targeted interviews, the report identifies those pre-existing cybersecurity challenges worsened by the impact of the pandemic crisis.

Key findings

85% of the SMEs surveyed agree that cybersecurity issues would have a serious detrimental impact on their businesses with 57% saying they would most likely go out of business.

Out of almost 250 SMEs surveyed, 36% reported that they had experienced an incident in the last 5 years. Nonetheless, cyberattacks are still not considered as a major risk for a large number of SMEs and a belief remains that cyber incidents are only targeting larger organisations.

However, the study reveals that phishing attacks are among the most common cyber incidents SMEs are likely to be exposed to, in addition to ransomware attacks, stolen laptops, and Chief Executive Officer (CEO) frauds.

For instance, with the concerns induced by the pandemic, cyber criminals seek to compromise accounts using phishing emails with Covid-19 as a subject.

CEO frauds are other decoys meant to lure an employee into acting upon the instructions of a fraudulent email displayed as if sent from their CEO, and usually requesting a payment to be performed in urgency under business-like circumstances.

The report unveils the following challenges SMEs are faced with:

- Low awareness of cyber threats;
- Inadequate protection for critical and sensitive information;

- Lack of budget to cover costs incurred for implementing cybersecurity measures;
- Availability of ICT cybersecurity expertise and personnel;
- Absence of suitable guidelines tailored to the SMEs sector;
- Moving online;
- Low management support.

How to address those challenges?

The recommendations issued fall into three categories:

People

People play an essential role in the cybersecurity ecosystem. The report draws attention to the importance of responsibility, employee buy-in and awareness, cybersecurity training and cybersecurity policies as well as third party management in relation to confidential and/or sensitive information.

Processes

Monitoring internal business processes include performing audits, incident planning and response, passwords, software patches and data protection.

Technical

At the technical level, a number of aspects should be considered in relation to network security, anti-virus, encryption, security monitoring, physical security and the securing of backups.

Number 8

Data of 700 million LinkedIn users reportedly advertised on dark web

National Cyber Security Centre

Data belonging to 700 million LinkedIn users has reportedly been advertised for sale on the dark web.

Based on a sample data set, security researchers found information relating to real accounts including users' full names, email addresses, phone numbers and physical addresses.

LinkedIn has posted an update about the reports, stating that this is not a data breach and its initial investigations have found the information was scraped from the internet. It said no private Linkedin member data had been exposed. You may visit:
https://news.linkedin.com/2021/june/an-update-from-linkedin

Affected LinkedIn users should still be vigilant against suspicious messages and phone calls relating to their scraped data. Cyber criminals are opportunistic and may use the recent news to trick people into clicking on scam messages.

The NCSC has produced guidance to help individuals spot suspicious messages and deal with them effectively, and more relevant advice on actions to take can be found in our data breaches guidance.

An update on report of scraped data

LinkedIn Pressroom

Our teams have investigated a set of alleged LinkedIn data that has been posted for sale. We want to be clear that this is not a data breach and no private LinkedIn member data was exposed.

Our initial investigation has found that this data was scraped from LinkedIn and other various websites and includes the same data reported earlier this year in our April 2021 scraping update.

Members trust LinkedIn with their data, and any misuse of our members' data, such as scraping, violates LinkedIn terms of service. When anyone tries to take member data and use it for purposes LinkedIn and our

members haven't agreed to, we work to stop them and hold them accountable.

For additional information about our policies and how we protect member data from misuse:
https://www.linkedin.com/help/linkedin/answer/56347/prohibited-software-and-extensions

Number 9

Thousands of fake online pharmacies shut down in INTERPOL operation

INTERPOL

A record number of fake online pharmacies have been shut down under Operation Pangea XIV targeting the sale of counterfeit and illicit medicines and medical products.

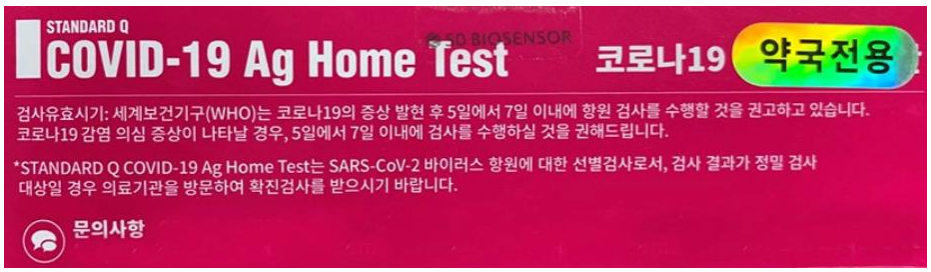
The operation coordinated by INTERPOL involved police, customs and health regulatory authorities from 92 countries.

It resulted in 113,020 web links including websites and online marketplaces being closed down or removed, the highest number since the first Operation Pangea in 2008.

In Venezuela a man was arrested after he developed an e-commerce platform on WhatsApp to sell illicit medicines.

In the UK, in addition to the seizure of some three million fake medicines and devices worth more than USD 13 million, authorities also removed more than 3,100 advertising links for the illegal sale and supply of unlicensed medicines, and shut down 43 websites.

Operation Pangea XIV also showed that criminals are continuing to cash in on the demand for personal protection and hygiene products generated by the COVID-19 pandemic.



Fake and unauthorized COVID-19 testing kits accounted for more than half of all medical devices seized during the week of action (18 – 25 May) which resulted in 277 arrests worldwide and the seizure of potentially dangerous pharmaceuticals worth more than USD 23 million.

In Italy, authorities recovered more than 500,000 fake surgical masks as well as 35 industrial machines used for production and packaging.

"As the pandemic forced more people to move their lives online, criminals were quick to target these new 'customers'," said INTERPOL Secretary General Jürgen Stock.

"Whilst some individuals were knowingly buying illicit medicines, many thousands of victims were unwittingly putting their health and potentially their lives at risk.

"The online sale of illicit medicines continues to pose a threat to public safety, which is why operations such as Pangea remain vital in combating this global health scourge," added Secretary General Stock.

"As crimes continue to evolve amidst the COVID-19 pandemic, the authorities must remain vigilant in dismantling criminal networks involved in the proliferation of illicit pharmaceutical products especially in online platforms," said the Head of the INTERPOL National Central Bureau in the Philippines, Allan C. Guisihan.

"Despite the official conclusion of this operation, the Philippines will continue to pursue its efforts in protecting the environment to ensure public health."

"Through Operation Pangea, we have supported INTERPOL, the UK's Medicines and Healthcare products Regulatory Agency and Border Force in tackling the worldwide threat of pharmaceutical crime linked to the COVID-19 pandemic.

We have seen how organized crime groups have responded to the changing environment however, we also continue to adapt and work with partners to disrupt their activities," said Kathryn Clarke Head of UK International Crime Bureau from the National Crime Agency.

Checks of some 710,000 packages led to the discovery of fake and illicit drugs hidden amongst legitimate products including clothes, jewellery, toys, food and baby products. In Qatar officials discovered 2,805 nerve pain tablets hidden inside tins of baked beans.

Supported by the Pharmaceutical Security Institute, the United Nations Office on Drugs and Crime/World Customs Organization's Container Control Programme and Europol, overall the operation resulted in the seizure of around 9 million medical devices and illicit pharmaceuticals, including:

- Hypnotic and sedative medication
- erectile dysfunction pills
- Medical devices (Covid Test kits, masks, syringes, catheters, surgical devices etc)
- analgesics/painkillers
- anabolic steroids
- antiseptics and germicides
- anti-cancer medication
- anti-malarials
- vitamins

To read more:
https://www.interpol.int/en/News-and-Events/News/2021/Thousands-of-fake-online-pharmacies-shut-down-in-INTERPOL-operation

Number 10

Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments

Executive summary

Since at least mid-2019 through early 2021, Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS), military unit 26165, used a Kubernetes cluster to conduct widespread, distributed, and anonymized brute force access attempts against hundreds of government and private sector targets worldwide.

GTsSS malicious cyber activity has previously been attributed by the private sector using the names Fancy Bear, APT28, Strontium, and a variety of other identifiers.

The 85th GTsSS directed a significant amount of this activity at organizations using Microsoft Office 365 cloud services; however, they also targeted other service providers and onpremises email servers using a variety of different protocols.

These efforts are almost certainly still ongoing.

This brute force capability allows the 85th GTsSS actors to access protected data, including email, and identify valid account credentials. Those credentials may then be used for a variety of purposes, including initial access, persistence, privilege escalation, and defense evasion.

The actors have used identified account credentials in conjunction with exploiting publicly known vulnerabilities, such as exploiting Microsoft Exchange servers using CVE 2020-0688 and CVE 2020-17144, for remote code execution and further access to target networks.

After gaining remote access, many well-known tactics, techniques, and procedures (TTPs) are combined to move laterally, evade defenses, and collect additional information within target networks.

Network managers should adopt and expand usage of multi-factor authentication to help counter the effectiveness of this capability. Additional mitigations to ensure strong access controls include time-out and lock-out features, the mandatory use of strong passwords, implementation of a Zero Trust security model that uses additional

attributes when determining access, and analytics to detect anomalous accesses.

Additionally, organizations can consider denying all inbound activity from known anonymization services, such as commercial virtual private networks (VPNs) and The Onion Router (TOR), where such access is not associated with typical use.

Description of targets

This campaign has already targeted hundreds of U.S. and foreign organizations worldwide, including U.S. government and Department of Defense entities. While the sum of the targeting is global in nature, the capability has predominantly focused on entities in the U.S. and Europe.

Types of targeted organizations include:

Known TTPs

The actors used a combination of known TTPs in addition to their password spray operations to exploit target networks, access additional credentials, move laterally, and collect, stage, and exfiltrate data, as illustrated in the

figure below. The actors used a variety of protocols, including HTTP(S), IMAP(S), POP3, and NTLM. The actors also utilized different combinations of defense evasion TTPs in an attempt to disguise some components of their operations; however, many detection opportunities remain viable to identify the malicious activity.

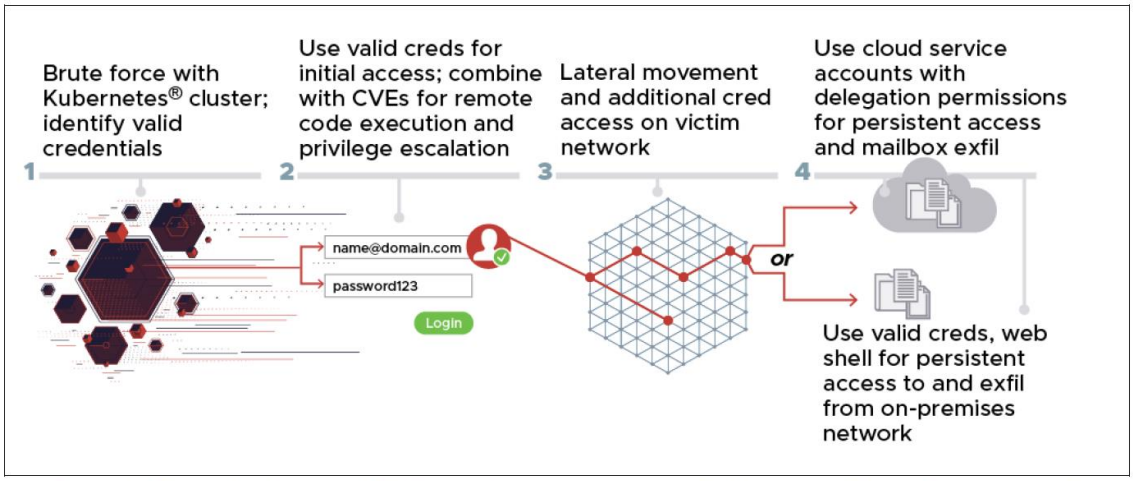


Figure 1: Example of several TTPs used together as part of this type of brute force campaign

To read more:
https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF

Disclaimer

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

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

This information:

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

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

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

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

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

- is in no way constitutive of an interpretative document;

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

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

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

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

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

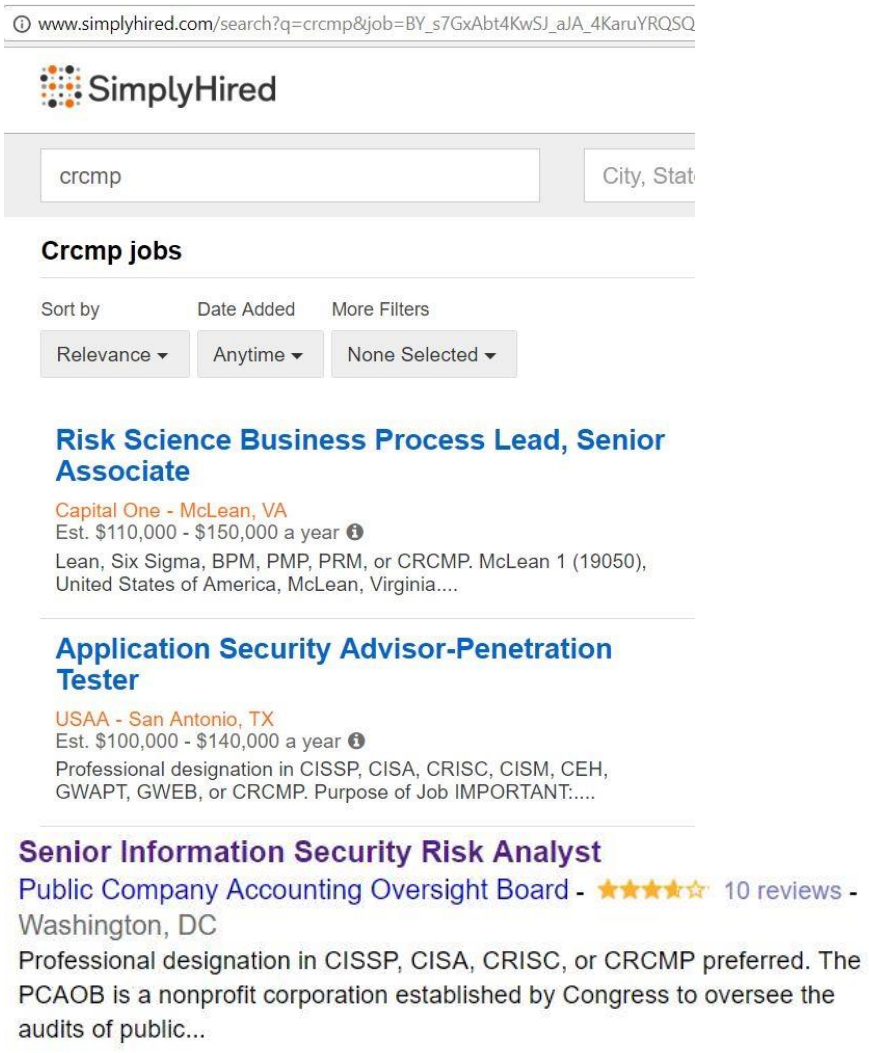
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

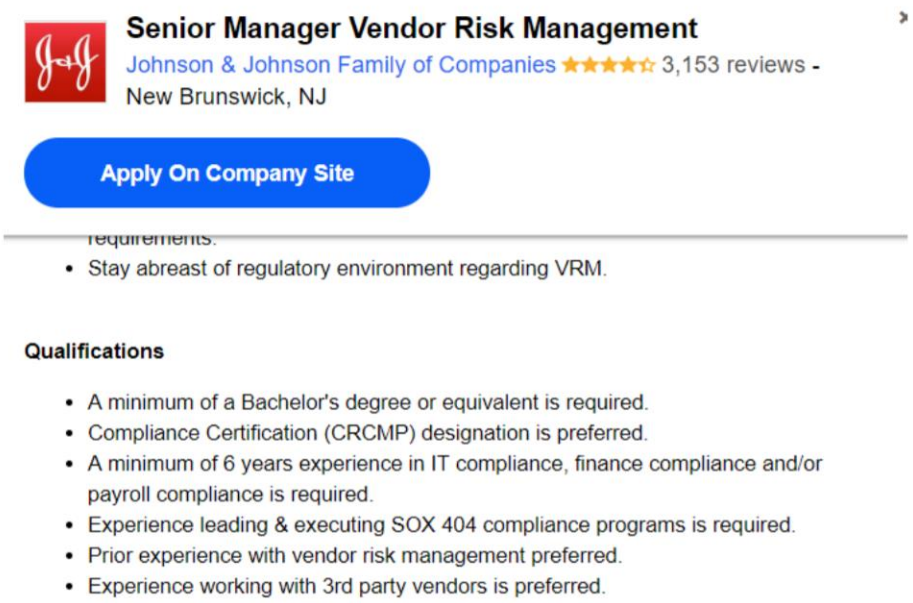
You can explore what we offer to our members:

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

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

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





Senior Manager Vendor Risk Management

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

Apply On Company Site

requirements.

- Stay abreast of regulatory environment regarding VRM.

Qualifications

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

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

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

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

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

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

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

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