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, May 24, 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 can the European National Competent Authorities (NCAs) *complement* the information obtained through the on-site inspections? Well, the answer is called *mystery shopping (MS)*.

According to the European Banking Authority (EBA), *mystery shopping* is understood as an *undercover* research approach used by NCAs, or market research companies that they may have used, to measure quality of customer service and/or gather information about financial products and services and the conduct of Financial Institutions (FIs) towards consumers.

MS may include the use of individuals who may act as potential or actual customers and who are trained and briefed to experience and measure key phases of a product's lifecycle and compliance with particular requirements. They report back their experiences in a detailed and

objective way. They perform specific tasks, for example reviewing how staff perform against pre-determined standards during an interaction with a customer.

That interaction may occur at the pre-contractual, contractual or post-contractual phase and may involve purchasing a product/service, asking questions, or registering complaints.

MS enables supervisors to carry out an assessment, in concrete situations, rather than relying on documents kept by firms, on-site interviews, or surveys.

This is interesting. The EBA was not the place to look for *covert human intelligence experts*, but things change.

You can read more at number 2 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 5)

2021 INSURANCE STRESS TEST

Number 2 (Page 7)

The European Banking Authority publishes report on mystery shopping activities of national authorities

Number 3 (Page 9)

Recommendations for the security of Connected and Automated Mobility (CAM)

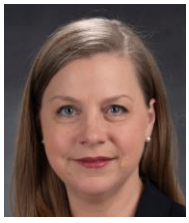
Number 4 (Page 12)

MAS Launches Global FinTech Hackcelerator for a Greener Financial Sector

Number 5 (Page 14)

The economic outlook and implications for monetary policy

Michelle W Bowman, Member of the Board of Governors of the Federal Reserve System, at The Colorado Forum, Denver, Colorado.



Number 6 (Page 20)

Monetary policy during Covid

Shann Memorial Lecture by Mr Guy Debelle, Deputy Governor of the Reserve Bank of Australia.

Number 7 (Page 23)

Commitment to sustainable reporting culture is key to Bangladesh banks' transparency and efficiency

Additional Managing Director at Standard Bank Limited (a Shari'ah Based Islami Bank in Bangladesh)

Number 8 (Page 24)

Further TTPs associated with SVR cyber actors

National Cyber Security Centre
a part of GCHQ

Number 9 (Page 26)

Colonial Pipeline
Media Statement Updated: Colonial Pipeline System Disruption

Colonial Pipeline Company

Number 10 (Page 27)

Researchers Demonstrate Sarcasm Detector for Online Communications

SocialSim researchers demonstrate deep learning model capable of accurately classifying sarcasm in textual communications, addressing online sentiment analysis roadblock

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 1

2021 INSURANCE STRESS TEST

The European Insurance and Occupational Pensions Authority (EIOPA) regularly conducts insurance stress tests to assess the resilience of the European insurance market in case of adverse financial and economic conditions and identify potential vulnerabilities in the insurance industry.

Stress tests are not a pass or fail exercise. The results are used to identify actions to minimise or mitigate identified risks.

SCENARIO

A prolonged COVID-19 scenario in a 'lower for longer' interest environment

SHOCKS:

The economic consequences of a prolonged economic contraction are translated in a set of market and insurance specific shocks.

ASSESSMENT:

Evaluate both the impact on the solvency and the liquidity position of the undertakings.

	Capital	Liquidity
Scenario	**Low-for-long in an adverse COVID aftermath** - Market shocks - Insurance specific shocks	
Approach	**Instantaneous shocks** **Fixed balance sheet** (no reactive Management Actions) **Constrained balance sheet** (with guided reactive Management Actions)	
Metrics	**Balance sheet based** (Excess of Assets over Liabilities) **Solvency based** (Own Funds, Solvency Capital Requirement)	**Net flow position over 90 days** (in-flows – out-flows) **Sustainability** of the net-flow position
Disclosure	**Aggregated** (stress test report): full set of balance sheet and solvency indicators **Individual:** subset of balance sheet indicators, **upon consent**	**Aggregated** (stress test report): set of indicators based on liquidity metrics

OBJECTIVES

› To assess the resilience of participants to unfavourable scenarios

› To consider possible recommendations to industry, leading to dialogue between supervisors and insurance undertakings on potential remedial actions;

› To complement the microprudential assessment with the estimation of potential spill-over from the insurance sector triggered by widespread reactions to the prescribed shocks.

To read more:
https://www.eiopa.europa.eu/content/2021-insurance-stress-test-factsheet_en

https://www.eiopa.europa.eu/insurance-stress-test-2021

https://www.eiopa.europa.eu/sites/default/files/financial_stability/insurance_stress_test/insurance_stress_test_2021/2021-stress-test-technical-specifications-v1.1.pdf

Number 2

The European Banking Authority publishes report on mystery shopping activities of national authorities

- This publication is the EBA's first step in the fulfilment of its new coordination mandate on mystery shopping activities of National Competent Authorities (NCAs);

- It summarises the most common approaches taken by NCAs on mystery shopping, presents some lessons learned, and identifies good practices;

- Mystery shopping allows NCAs to obtain greater insight into the conduct of financial institutions. The latter are then encouraged to take corrective actions and to better comply with applicable requirements, thus eventually enhancing the protection of consumers.

The European Banking Authority (EBA) published a Report on the mystery shopping activities of NCAs. The EBA collated mystery shopping activities by NCAs with a view to share experiences, learn valuable lessons, and identify good practices for the benefit of the EBA and NCAs that use or intend to use mystery shopping in the future.

The Report covers mystery shopping initiatives of NCAs in respect of products that fall within the scope of action of the EBA's consumer protection mandate, which are consumer credit, mortgage credit, deposits, payment services, electronic money, and payment accounts.

It summarises the most common approaches used by the NCAs, based on the information collated primarily covering the period from 2015 to 2020.

It does so by reviewing three key characteristics of mystery shopping activities: their objective, subject matter and product scope, the methodologies used by NCAs, and the follow-up actions after the mystery shopping was concluded. The Report also identify some lessons learned and sets out good practices.

At this stage, only a limited number of NCAs carried out such mystery shopping activities in their jurisdiction. Moreover, some NCAs reported that discussions are currently taking place at national level on the possibility of adding such powers to relevant competent authorities' mandate, for some of them as part of the implementation of the EU Consumer Protection Cooperation Regulation.

Regarding the lessons learned, the Report explains that mystery shopping allows NCAs to obtain greater insight into the conduct of financial institutions.

This, in turn, encourages them to take corrective actions better to comply with applicable requirements, and eventually enhances the protection of consumers.

Among the good practices identified by the NCAs, most of them concern common procedural aspects such as organising training for NCAs' inspection and supervisory staff, identifying target customer profiles, and defining agreed 'rules' of customer's behaviour.

To read more:
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2021/1000492/EBA%20Report%20on%20the%20mystery%20shopping%20activities%20of%20National%20Competent%20Authorities.pdf

Contents

List of abbreviations 3

Executive summary 4

1. Background 6

2. Mystery shopping activities of National Competent Authorities 10

2.1 Objective, subject matter and product scope 10

2.2 Methodologies used 11

2.3 Follow-up actions after the mystery shopping 16

3. Lessons learned 18

3.1 Main benefits 18

3.2 Main challenges 19

3.3 Good practices identified by National Competent Authorities 19

Number 3

Recommendations for the security of Connected and Automated Mobility (CAM)

The Connected and Automated Mobility (CAM) sector is an entire ecosystem of services, operations and infrastructures comprised of a variety of actors and stakeholders.

Under a new regulation set by the United Nations, car manufacturers are required to secure vehicles against cyberattacks.

In the European Union, the new regulation on cybersecurity will be mandatory for all new vehicle types from July 2022 and will become mandatory for all new vehicles produced from July 2024.

Moreover, the UNECE Regulation and related ISO standards apply to all CAM stakeholders who must ensure that their products and services conform to cybersecurity goals.

Increased connectivity and technological development in the ecosystem through various services, components and technologies are continuously expanding.

Therefore, within the CAM sector, where innovation and market growth are expanding, global players in the CAM sector face a risk of cyberattacks.

Connected services may be attacked by cyber-attackers and create cyber fraud, data breach and privacy incidents, as well as software overrides resulting in dangerous situations and accidents when part of the vehicle to everything (V2X) network is attacked, thereby threatening the drivers, road users and companies.

Efforts across the whole industry should be made to ensure that even if one system is compromised and/or tampered, the rest of the systems remain unaffected.

The interlinking of systems and services (both inside and outside the vehicle) and thus intelligent and connected mobility are already revolutionising users' lives.

The whole ecosystem involved in the CAM lifecycle has to cope with key challenges that add complexity to responding and managing CAM cybersecurity risks.

Today, connected vehicles, connected environment and connected infrastructure should be designed with new capabilities and features that have the potential to provide increased safety, better vehicle performance, competitive digital products and services, more comfort, environmental friendliness, as well as convenience for its end-users.

Governments, manufacturers, private companies (incl. SMEs and start-ups) as well as IT enterprises are all involved in the future development of intelligent and connected and automated mobility.

Fixed and mobile telecommunication infrastructure is necessary for cars to communicate with the smart road infrastructure (I2V and V2I), with devices (V2D), between vehicles (V2V), with other networks such as access to cloud infrastructure (V2N) as well as within the vehicle.
The aim of this report is to provide a high-level overview of the cybersecurity challenges in the CAM sector and to highlight both the concerned CAM actors and associated recommendations.

Cybersecurity in the CAM ecosystem is partially standardised and the role of standards is widely recognised.

All stakeholders' contributions to the CAM ecosystem are intertwined. Standards and regulations are often not adopted uniformly worldwide, and therefore some countries may advance faster than others in building a safe and secure cybersecurity system around CAM infrastructure.

In the context of growing cybersecurity threats and concerns about cybersecurity and data protection, this report aims to identify the main challenges in the current situation and to propose actionable recommendations for the different stakeholders involved in the CAM ecosystem to enhance the level of security and resilience of CAM infrastructures and systems in Europe.

Challenges in the CAM ecosystem arise from the whole lifecycle, therefore this report points to detailed challenges that the stakeholders are facing across Europe.

The recommendations proposed by ENISA aim to guide all CAM ecosystem stakeholders and to contribute to the improvement and harmonisation of cybersecurity in the CAM ecosystem in the European Union.

Using a layered approach of primary and secondary research, this report summarises insights across a complex CAM ecosystem.

Primary research methods included a survey and a series of interviews and validation discussions with key stakeholders from the CAM ecosystem.

Secondary research methods included desktop research of works of ENISA, official statistics, academic research, external studies and official documents, white papers, legislation, policies, strategies and initiatives to identify challenges and lessons learnt on cyber incidents against the CAM ecosystem.

To read more:
https://www.enisa.europa.eu/publications/recommendations-for-the-security-of-cam

Figure 1: Cybersecurity Challenges in the CAM area

Number 4

MAS Launches Global FinTech Hackcelerator for a Greener Financial Sector

Monetary Authority of Singapore

The Monetary Authority of Singapore (MAS) announced the launch of the 6th edition of the Global FinTech Hackcelerator, with the theme "Harnessing Technology to Power Green Finance".

The competition, supported by Oliver Wyman, seeks to unlock the potential of FinTech in accelerating the development of green finance in Singapore and the region.

FinTech firms and solution providers around the world are invited to submit innovative solutions to address over 50 problem statements that have been collected from financial institutions and green finance industry players.

These problem statements focus on three key challenges:

(i) Mobilising Capital;
(ii) Monitoring Commitment; and
(iii) Measuring Impact.

Up to 15 finalists will be shortlisted for a virtual programme where they will be paired with a Corporate Champion to develop customised prototypes on the API Exchange (APIX).

Each finalist will also receive a S$20,000 cash stipend and be eligible for a fast-tracked application for the MAS Financial Sector Technology and Innovation Scheme Proof-of-Concept Grant of up to S$200,000.

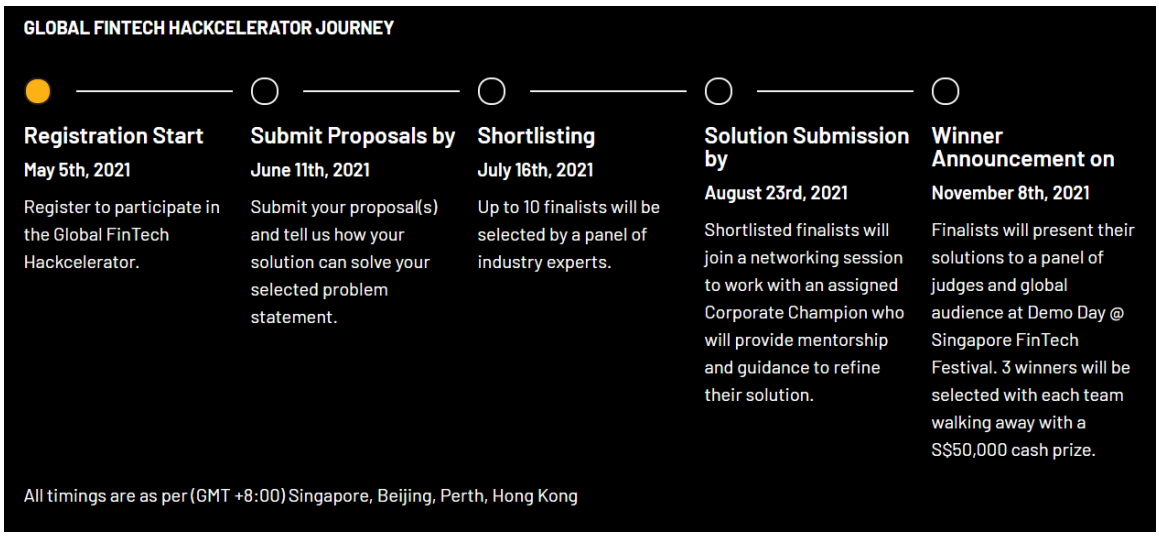
Finalists will pitch their solutions at the Demo Day held at this year's Singapore FinTech Festival. Up to three winners will be selected, with each receiving S$50,000 in prize money.

Mr Sopnendu Mohanty, Chief FinTech Officer of MAS said, "Green FinTech can be an important enabler to accelerate Asia's transition to a low carbon future.

It can provide much needed innovative solutions, and develop the crucial technology stack, which can help promote green financial services, catalyse efficient allocation of green capital, and facilitate trust in the green data

value chain. I encourage all innovators to make use of this platform and showcase their Green FinTech solutions to the world."

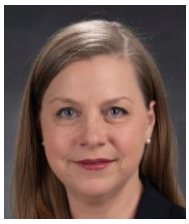
All FinTech firms and solution providers are encouraged to submit their applications for the MAS Global FinTech Hackcelerator by 11 June 2021 at: https://hackolosseum.apixplatform.com/hackathon/gfh2021



Number 5

The economic outlook and implications for monetary policy

Michelle W Bowman, Member of the Board of Governors of the Federal Reserve System, at The Colorado Forum, Denver, Colorado.



Thank you for this opportunity to address the members of the Colorado Forum, which has been an arena for thoughtful discussion and debate for more than 40 years.

Today I would like to discuss a subject that I expect is of great interest to Coloradans and others: the outlook for the U.S. economy in 2021.

I believe that the economy has gained momentum in the past several months and is well positioned to grow strongly in 2021.

Nevertheless, we have further to go to recover from the economic damage inflicted by the COVID-19 pandemic, and risks remain.

As we all know, starting in late February or March of last year, widespread economic and social lockdowns and other effects of the pandemic caused the swiftest and deepest contraction in employment and economic activity since the Great Depression.

Money markets, the Treasury market, and other parts of the financial system seized up, and there were fears of another severe financial crisis.

The Federal Reserve stepped in quickly to assist, reviving several lending facilities used in the previous crisis and creating several new facilities.

We also cut short-term interest rates to near zero and began purchasing large quantities of Treasury and agency securities to help sustain the flow of credit to households and businesses.

Congress and the Administration also worked together to provide effective and timely support.

Calm was restored in financial markets, and employment and output began growing in May, but it was a very deep hole to fill.

Since that time, progress in controlling the pandemic has been a dominant force driving the economic recovery.

Rapid progress last summer gave way to slower economic growth over the turn of the year, as infection rates once again surged.

But after a substantial pickup in vaccinations and steep declines in virus-related hospitalizations and deaths, the economic outlook has brightened. Job creation had stalled over the winter months but improved again starting in February.

Over the past year, we've seen a return of nearly 14 million jobs.

Another significant factor contributing to the recovery is the resilience of private-sector businesses.

Our economic recovery has been more rapid and stronger than many forecasters expected, partly due to the ability of businesses to adapt to conditions that none of them had planned for, and few even imagined could be possible.

Initially, government assistance was important, but millions of businesses were at risk of closure.

Instead, many are open and growing today due to the resourcefulness and determination of entrepreneurs and workers and their ability to adjust business plans and operations to deal with the effects of social-distancing and operating restrictions.

Of course, technology helped a great deal, but businesses were able to find many other ways to maintain operations and sustain their connections to customers.

In writing the history of these eventful times, I hope that the efforts of these businesses and the strength of America's market-based economy get the considerable credit they deserve.

Recently, the incoming data indicate that economic activity is on an upswing, and the risks of more negative outcomes-especially those from COVID-19-appear to be easing.

Vaccinations and the easing of operating and social-distancing restrictions are boosting consumer and business confidence, with the results clear to see in the data on spending.

Retail sales surged nearly 10 percent in March and are actually above the trendline that was interrupted by the pandemic a year ago.

One particularly encouraging signal in that report was a sharp expansion in spending on food services.

I hope this is an indication that consumers are finally returning to in-person dining as spring arrives and local authorities allow restaurants to accommodate more diners.

If so, and my fingers are crossed, it is a very good sign of further progress in one of the sectors hardest hit by the pandemic.

In the job market, job gains rebounded to 916,000 in March. At our March meeting, my view was broadly in line with the median of projections of other members of the Federal Open Market Committee (FOMC), which anticipated the economy would grow between 5.8 percent and 6.6 percent in 2021.

But the outlook has improved since then, and it now appears that real gross domestic product may increase close to or even above the higher end of that range. This annual increase would be the largest in 36 years.

Likewise, the FOMC median in March was for unemployment to fall to 4.5 percent at the end of 2021, and now it seems possible that it may fall even further. With the economy continuing to reopen, I expect the pace of job creation to remain unusually strong over the spring and summer.

Over the past few months many schools have resumed some form of in-person learning, which should translate into a rebound in labor force participation as more parents overseeing virtual education and child care are able to increase hours or return to the workforce.

The biggest risk to the outlook continues to be the course of the pandemic. I see good reasons to be optimistic.

Vaccinations are proceeding at a rapid pace, and this progress is supporting decisions by state and local leaders to relax economic restrictions.

Most importantly, deaths related to the virus have continued to fall steadily and are at roughly the rate as in early October of last year.

I remain hopeful that progress in the economic recovery can stay ahead of new challenges that might emerge, like the spread of new virus variants.

That would allow states and localities to continue easing economic and social distancing restrictions and encourage consumers and businesses to return to normal activities.

I understand that in Colorado, for example, officials are considering lifting social-distancing restrictions on individuals and businesses.

I would be interested to hear from this group about how businesses in Colorado have been faring and whether they have seen an improvement in demand as the pandemic conditions are easing.

While I am optimistic about the ongoing recovery, one lesson of the past year is the significant degree of uncertainty about the course of the virus and its effect on the economy.

We experienced periods of considerable progress last year, but we saw some of that progress overtaken by waves of the infection late in the year.

Likewise, economic growth rebounded much more quickly than many had expected, but then slowed late in 2020 before regaining speed following the availability of the vaccine.

Even with recent encouraging reports on food services, activity in the travel, leisure, and hospitality sectors is still severely compromised, but is showing glimmers of activity.

It may be some time before we know whether old habits will resume or new habits have developed that may define a post-pandemic new normal.

As I noted in a recent speech, I am particularly concerned about the longer-term effect on small businesses, many of which have held on with government aid and loan forbearance programs that will soon expire.

It will be several months before we know the final count of permanent small business closures from 2020, but it could be more than we expect.

I will now turn to how the Federal Reserve is proceeding in light of the strong signals of momentum building in the economy.

The economic recovery is not yet complete, and the uncertain course of the pandemic still presents risks in the near term, which is why my colleagues and I on the FOMC decided last week to maintain our highly accommodative stance of monetary policy.

Despite the progress to date and the signs of acceleration in the recovery, employment is still considerably short of where it was when the pandemic disrupted the economy and it is well below where it should be, considering the pre-pandemic trend.

In particular, our maximum employment mandate is intended as a broad and inclusive goal increasing employment and opportunity, but I remain concerned that employment gains for some minority groups have lagged behind those of others.

While job creation has been and is expected to remain strong, the pace will eventually slow as the share of those who have been unemployed for the longer-term increases among those who are looking for work.

We are making good progress toward our full employment goal, but we still have a long way to go, and risks remain.

This brings me to the other side of our policy mandate. Over the next several months, I expect that headline inflation measures will move above our long-run target of 2 percent.

A main reason I expect this outcome is simply the fact that the very low inflation readings during last spring's deep economic contraction will drop from the usual calculation of 12-month price changes.

But in addition, the unusually rapid rebound in economic activity that we've seen, along with the pandemic-driven shift towards goods purchases, has led to supply-chain bottlenecks in a number of areas, which in turn have pushed up prices for many goods.

One prominent example is with semiconductor producers and their need to dramatically alter the mix of production to meet demands of the high-tech and automotive industries.

Although I expect these upward price pressures to ease after the temporary supply bottlenecks are resolved, the exact timing of that dynamic is uncertain.

If the supply bottlenecks prove to be more long-lasting than currently expected, I will adjust my views on the inflation outlook accordingly.

At this point, the risk that inflation remains persistently above our long-run target of 2 percent still appears small.

In summary, let me say that I am encouraged by the recent pace of the economic recovery, and I remain optimistic that this strength will continue in the coming months.

One reason for my optimism is that businesses have been effective in responding to the challenges posed by the pandemic and by economic restrictions implemented in efforts to contain it.

We really can't know how the pandemic will proceed and how that will affect the U.S. economy, but I think we are currently on a good path, and our policy is in a good place.

Thank you again for inviting me to speak to you today, and I would be happy to respond to your questions.

Number 6

Monetary policy during Covid

Shann Memorial Lecture by Mr Guy Debelle, Deputy Governor of the Reserve Bank of Australia.

Thank you for the opportunity to speak to you tonight. I am honoured to be giving the Shann lecture.

Edward Shann's work had a lasting impact on Australian economic thought.

As an economic historian, Shann looked to the past to inform solutions to the most important problems of his time, including how to lift Australia out of the Great Depression.

Many of Shann's key contributions seem orthodox today but were well ahead of his time.

Shann advocated for the removal of tariffs, a shift away from centralised wage fixing and a move to a more flexible exchange rate.

Shann also saw an important role for an independent central bank to prevent and respond to crises.

He was widely regarded as an excellent teacher, who left a significant impact on his students.

One such student was HC 'Nugget' Coombs, the Reserve Bank's first Governor. Coombs described Shann as 'supremely capable of communicating the excitement of intellectual exploration ... and establishing the sense of social responsibility, which should guide those who work in academic fields'.

Taking inspiration from Shann, tonight I will talk to you about the role the Reserve Bank has played in responding to the current crisis.

I will describe what the Reserve Bank has done over the past year to support the economy through the COVID pandemic.

I will talk about why we have taken these actions and some of the thinking behind the policy decisions.

Then I will look at the outcomes of these policy actions to date.

Finally, I will highlight some of the issues the Bank will be thinking about in the period ahead.

Policy actions during COVID

The Reserve Bank of Australia (RBA) has taken a number of complementary policy actions to support the Australian economy since the onset of COVID.

The RBA has lowered its policy interest rate to near zero, set a target for the 3-year government bond yield, enhanced its forward guidance commenced a program of purchasing government bonds and provided long-term low-cost funding to the banking system.

I will explain each of these actions in more detail shortly.

The overall aim of all these monetary policy actions has been to support economic activity in Australia through a number of channels.

The policy actions have underpinned record low funding costs across the financial system and for governments.

Lower borrowing costs free up cash flow for both households and businesses, some of which is spent.

The lower interest rates and the funding for the banking system support the flow of credit to households and businesses.

Lower interest rates also support asset prices, which boost balance sheets, and thereby consumption and investment.

Finally, a lower structure of interest rates leads to a lower value of the Australian dollar than would otherwise be the case.

The end result is a stronger Australian economy. The policy response has evolved over the pandemic period as information about the extent of the pandemic and its economic impact has unfolded.

The initial policy decisions were taken in March 2020, including at an unscheduled policy meeting on 18 March.

Further measures were announced in September and November 2020 and in February 2021.

In mid March 2020, as the impact of the virus and the health policy actions on the Australian economy became evident, the Reserve Bank Board put in place a comprehensive package at an unscheduled meeting to support jobs, incomes and businesses, so that when the health crisis receded, the country was well placed to recover strongly.

The package comprised:

- a reduction in the cash rate target (the policy interest rate) to 25 basis points, having already reduced the cash rate to 50 basis points at the earlier March Board meeting

- forward guidance that the Board will not increase the cash rate target until progress is being made towards full employment and it is confident that inflation will be sustainably within the 2–3 per cent target band

- reducing the interest rate paid on Exchange Settlement (ES) balances (the balances the banking system holds with the RBA) to 10 basis points

- the introduction of a target on the 3-year Australian Government bond yield of around 25 basis points

- the purchase of bonds to address the dysfunction in the Australian government bond market

- a Term Funding Facility (TFF) for the banking system under which funds equivalent to 3 per cent of lending could be borrowed from the RBA for 3 years at 25 basis points (against eligible collateral) up until end September 2020. The TFF provided additional incentives to support lending to businesses, particularly small and medium-sized businesses

- the continued use of the RBA's open market operations to make sure that the financial system had a high level of liquidity. The RBA had already been expanding its liquidity provision prior to the mid-March Board meeting to address the growing dislocation in financial markets.

To read more: https://www.bis.org/review/r210506a.pdf

Number 7

Commitment to sustainable reporting culture is key to Bangladesh banks' transparency and efficiency

Additional Managing Director at Standard Bank Limited (a Shari'ah Based Islami Bank in Bangladesh)

Sustainability reporting is mandatory for banking institutions in Bangladesh considering environmental and socio-economic and governance issues

- Banks' commitment to a healthy sustainable disclosure practice is good for everyone

- Bangladeshi banks are bound by policies to incorporate 'green banking' initiatives in their agenda

- Majority of banks do not practice sustainability reporting

A sustainable world economy is essential for society, and a bank, as responsible corporate citizen, needs to devise a long-term strategy towards sustainable financing activities through various effective initiatives. The question is, "How can it be started?"

To read more:
https://www.theasianbanker.com/updates-and-articles/commitment-to-sustainable-reporting-culture-is-key-to-bangladesh-banks-transparency-and-efficiency

Number 8

Further TTPs associated with SVR cyber actors

This report provides further details of Tactics, Techniques and Procedures (TTPs) associated with SVR cyber actors. SVR cyber actors are known and tracked in open source as APT29, Cozy Bear, and the Dukes.

UK and US governments recently attributed SVR's responsibility for a series of cyber-attacks, including the compromise of SolarWinds and the targeting of COVID-19 vaccine developers.

Alongside this attribution, the United States' National Security Agency (NSA), Federal Bureau of Investigation (FBI), and Cybersecurity and Infrastructure Security Agency (CISA) released an advisory detailing the exploits most recently used by the group.

The FBI, Department of Homeland Security (DHS) and CISA also issued an alert providing information on the SVR's cyber tools, targets, techniques and capabilities. The SVR is Russia's civilian foreign intelligence service.

The group uses a variety of tools and techniques to predominantly target overseas governmental, diplomatic, think-tank, healthcare and energy targets globally for intelligence gain.

The SVR is a technologically sophisticated and highly capable cyber actor.

It has developed capabilities to target organisations globally, including in the UK, US, Europe, NATO member states and Russia's neighbours.

The NCSC, NSA, CISA and CSE previously issued a joint report regarding the group's targeting of organisations involved in COVID-19 vaccine development throughout 2020 using WellMess and WellMail malware.

SVR cyber operators appear to have reacted to this report by changing their TTPs in an attempt to avoid further detection and remediation efforts by network defenders.

These changes included the deployment of the open-source tool Sliver in an attempt to maintain their accesses.

The group has also been observed making use of numerous vulnerabilities, most recently the widely reported Microsoft Exchange vulnerability.

To read more:
https://www.ncsc.gov.uk/files/Advisory%20Further%20TTPs%20associated%20with%20SVR%20cyber%20actors.pdf

Tactic	Technique	Procedure
Reconnaissance	T1595.002: Active Scanning	SVR frequently scans for publicly available exploits, most recently including Microsoft Exchange servers vulnerable to CVE-2021-26855.
Initial Access	T1190: Exploit Public-Facing Application	SVR frequently uses publicly available exploits to conduct widespread exploitation of vulnerable systems, including against Citrix, Pulse Secure, FortiGate, Zimbra and VMWare.
	T1195.002: Supply Chain Compromise: Compromise Software Supply Chain	SVR target organisations who supply privileged software to intelligence targets.
	T1199: Trusted Relationship	SVR leveraged access gained from the SolarWinds campaign to compromise a certificate issued by Mimecast, which it then used to authenticate a subset of Mimecast's products with customer systems.
Execution	T1059.005: Command and Scripting Interpreter: Visual Basic	SVR deployed Sibot, a simple custom downloader written in VBS, after compromising victims via SolarWinds.
Persistence	T1505.003: Server Software Component: Web Shell	SVR typically deploy a web shell on Microsoft Exchange servers following successful compromise.
	T1078: Valid Accounts	SVR actors have maintained persistence on high value targets using stolen credentials.

Number 9

Colonial Pipeline
Media Statement Updated: Colonial Pipeline System Disruption

On May 7, the Colonial Pipeline Company learned it was the victim of a cybersecurity attack. We have since determined that this incident involves ransomware.

In response, we proactively took certain systems offline to contain the threat, which has temporarily halted all pipeline operations, and affected some of our IT systems.

Upon learning of the issue, a leading, third-party cybersecurity firm was engaged, and they have launched an investigation into the nature and scope of this incident, which is ongoing. We have contacted law enforcement and other federal agencies.

Colonial Pipeline is taking steps to understand and resolve this issue. At this time, our primary focus is the safe and efficient restoration of our service and our efforts to return to normal operation.

This process is already underway, and we are working diligently to address this matter and to minimize disruption to our customers and those who rely on Colonial Pipeline.

Number 10

Researchers Demonstrate Sarcasm Detector for Online Communications

SocialSim researchers demonstrate deep learning model capable of accurately classifying sarcasm in textual communications, addressing online sentiment analysis roadblock

Sentiment analysis – the process of identifying positive, negative, or neutral emotion – across online communications has become a growing focus for both commercial and defense communities.

Understanding the sentiment of online conversations can help businesses process customer feedback and gather insights to improve their marketing efforts.

From a defense perspective, sentiment can be an important signal for online information operations to identify topics of concern or the possible actions of bad actors.

The presence of sarcasm – a linguistic expression often used to communicate the opposite of what is said with an intention to insult or ridicule – in online text is a significant hindrance to the performance of sentiment analysis.

Detecting sarcasm is very difficult owing largely to the inherent ambiguity found in sarcastic expressions.

“Sarcasm has been a major hurdle to increasing the accuracy of sentiment analysis, especially on social media, since sarcasm relies heavily on vocal tones, facial expressions, and gestures that cannot be represented in text,” said Brian Kettler, a program manager in DARPA’s Information Innovation Office (I2O). “Recognizing sarcasm in textual online communication is no easy task as none of these cues are readily available.”

Researchers from the University of Central Florida working on DARPA’s Computational Simulation of Online Social Behavior (SocialSim) program are developing a solution to this challenge in the form of an AI-enabled “sarcasm detector.”

The researchers have demonstrated an interpretable deep learning model that identifies words from input data – such as Tweets or online messages – that exhibit crucial cues for sarcasm, including sarcastic connotations or negative emotions.

Using recurrent neural networks and attention mechanisms, the model tracks dependencies between the cue-words and then generates a classification score, indicating whether or not sarcasm is present.

“Essentially, the researchers’ approach is focused on discovering patterns in the text that indicate sarcasm.

It identifies cue-words and their relationship to other words that are representative of sarcastic expressions or statements,” noted Kettler.

The researchers’ approach is also highly interpretable, making it easier to understand what’s happening under the “hood” of the model.

Many deep learning models are regarded as “black boxes,” offering few clues to explain their outputs or predictions.

Explainability is key to building trust in AI-enabled systems and enabling their use across an array of applications.

Existing deep learning network architectures often require additional visualization techniques to provide a certain level of interpretability.

To avoid this, the SocialSim researchers employed inherently interpretable self-attention that allows elements in the input data that are crucial for a given task to be easily identified.

The researchers’ capability is also language agnostic so it can work with any language model that produces word embeddings.

The team demonstrated the effectiveness of their approach by achieving state-of-the-art results on multiple datasets from social networking platforms and online media.

The model was able to successfully predict sarcasm, achieving a nearly perfect sarcasm detection score on a major Twitter benchmark dataset as well as state-of-the-art results on four other significant datasets.

The team leveraged publicly available datasets for this demonstration, including a Sarcasm Corpus V2 Dialogues dataset that is part of the Internet Argument Corpus as well as a news headline dataset from the Onion and HuffPost.

DARPA’s SocialSim program is focused on developing innovative technologies for high-fidelity computational simulation of online social behavior.

A simulation of the spread and evolution of online information could enable a deeper and more quantitative understanding of adversaries' use of the global information environment.

It could also aid in efforts to deliver critical information to local populations during disaster relief operations, or contribute to other critical missions in the online information domain.

Accurately detecting sarcasm in text is only a small part of developing these simulation capabilities due to the extremely complex and varied linguistic techniques used in human communication.

However, knowing when sarcasm is being used is valuable for teaching models what human communication looks like, and subsequently simulating the future course of online content.

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.

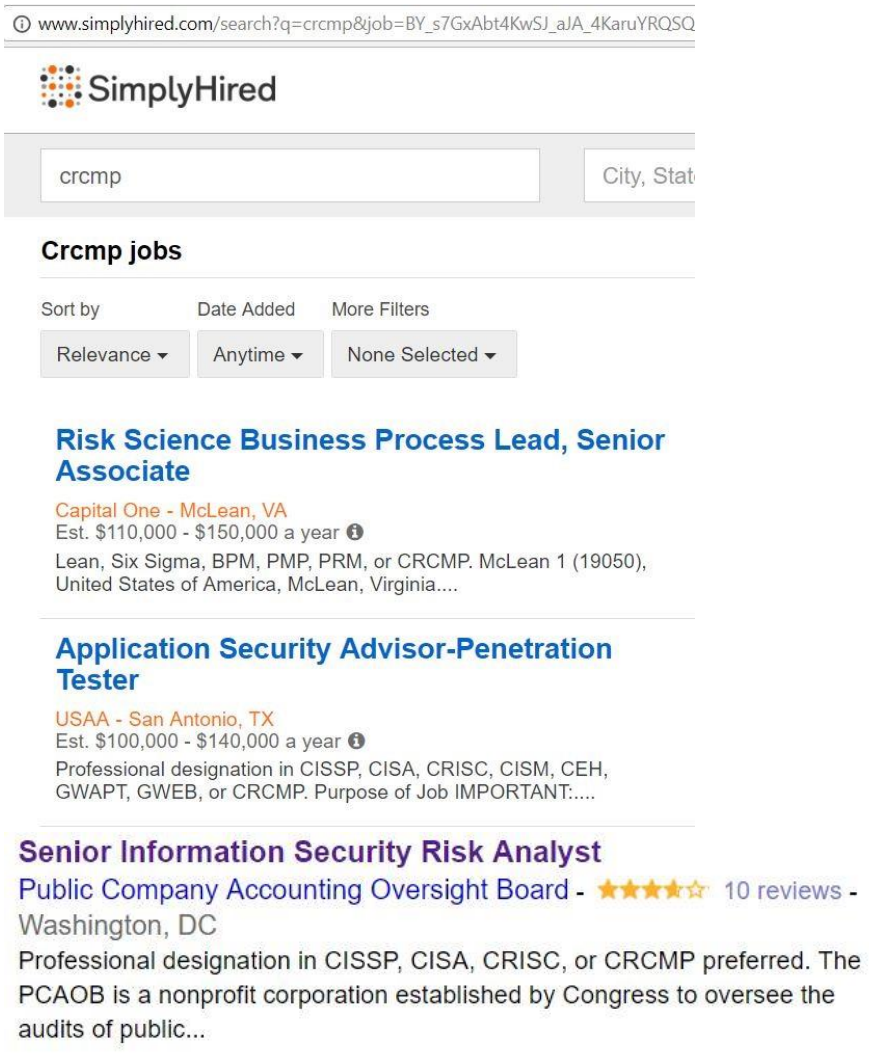
International Association of Risk and Compliance Professionals

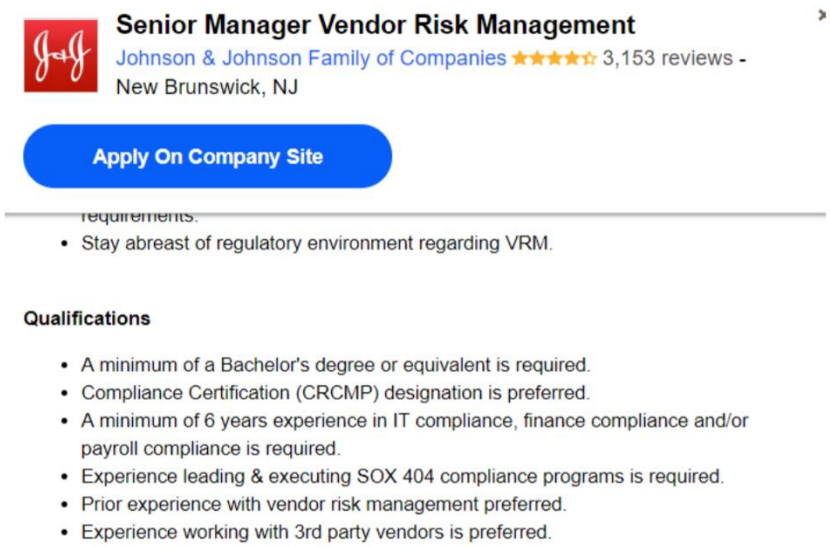
You can explore what we offer to our members:

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 around the world 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.