Monday, May 4, 2020

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

Dear members and friends,

I have just read that *rare events are highly unlikely; they may occur in exceptional circumstances*. As we neither have a common definition of the term *exceptional,* nor historical records and data to rely on, the probabilities or *rare events* are usually estimated subjectively.

In high impact / low likelihood events, like hurricane Katrina and the Fukushima disaster, risk probability is inherently difficult to assess.

According to the Bank for International Settlements, the coronavirus (Covid-19) pandemic is a *rare type of shock* to the world economy.

Its sudden and massive impact on activity comes at a time when the legacy of the Great Financial Crisis (GFC) of 2007–09 is still weighing on public and private sector balance sheets.

As its fallout will extend well beyond the removal of health-related restrictions, the subsequent economic recovery may be drawn-out.

So far, the economic policy response has primarily involved the decisive use of monetary and fiscal tools. For their part, prudential authorities have sought to support the flow of credit to firms, households and governments, most notably by relaxing banks' constraints on the use of liquidity and capital buffers.

A *release of buffers* can complement and enhance the effect of fiscal and monetary policies, provided that banks are both able and willing to expand their balance sheets.

For one, this means that markets' and management's assessment of what is a prudent buffer size should not prevent banks from lending.

In addition, banks should see greater value in using balance sheet capacity for lending rather than for discretionary payouts: a trade-off affected by the extent of risk-sharing with the public sector.

Banks need to *continue supporting* economic performance in the medium term, ie the period after the lifting of stringent health-related restrictions. This is not a given. The recession will bring about large losses that will materialise only gradually.

To avoid amplifying stress, banks will need buffers to absorb elevated losses for as long as the slump persists. After that, banks will still need buffers that they can draw upon in order to facilitate the rebound as robust counterparties and reliable intermediaries.

Welcome to the Top 10 list.

Best regards,

George Lekatis

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

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Number 6 (Page 19)

PCAOB Posts Request for Comment, Seeks Stakeholder Input on Critical Audit Matters

PCAOB
Public Company Accounting Oversight Board

Number 7 (Page 21)

Statement on principles to mitigate the impact of Coronavirus/COVID-19 on the occupational pensions sector

eiopa
European Insurance and Occupational Pensions Authority

Number 8 (Page 24)

Protecting healthcare and human rights organizations from cyberattacks

Tom Burt - Corporate Vice President, Customer Security & Trust

Microsoft

Number 9 (Page 29)

SEC Awards Over $27 Million to Whistleblower

Amounts Awarded to Whistleblowers by SEC Now Exceed $400 Million

Number 10 (Page 31)

FBI Warns of Advance Fee and BEC Schemes Related to Procurement of PPE and Other Supplies During COVID-19 Pandemic

Number 1

Macroeconomic effects of Covid-19: an early review

Frederic Boissay and Phurichai Rungcharoenkitkul

BIS

- Past epidemics had long-lasting effects on economies through illness and the loss of lives, while Covid19 is marked by widespread containment measures and relatively lower fatalities among young people.

- The short-term costs of Covid-19 will probably dwarf those of past epidemics, due to the unprecedented and synchronised global sudden stop in economic activity induced by containment measures.

- The current estimated impact on global GDP growth for 2020 is around –4%, with substantial downside risks if containment policies are prolonged. Output losses are larger for major economies.

The Covid-19 pandemic is not only the most serious global health crisis since the 1918 Great Influenza (Spanish flu), but is set to become one of the most economically costly pandemics in recent history.

Experience with past epidemics provides some insights into the various channels through which economic costs could arise, in the short as well as longer term.

At the same time, Covid-19 differs from previous episodes in several important ways.

Notably, the globally synchronised lockdowns and trauma of financial markets reinforce one another into an unprecedented economic sudden stop.

For these reasons, the Covid-19 global recession is unique.

However, past epidemics can shed light on transmission channels to the economy, especially when stringent containment policies are not in place.

This Bulletin provides an early review of empirical studies on the economic costs of epidemics.

We first review studies on past epidemics, and then turn to the latest quantitative estimates of Covid-19's impact on global growth.

Gauging short-term economic impact of Covid-195

While no two epidemics are exactly alike, the current pandemic differs fundamentally from past episodes.

The rapid global spread of Covid-19, aided by closer international integration and the possibility of transmission through carriers without symptoms, has led to much faster transmission than past episodes such as SARS.

This has prompted a large-scale containment policy, put in place globally in an almost synchronised way, in turn leading to a global sudden stop in economic activity.

How is this time different? Table 2

Factors	1918 pandemic	SARS	Covid-19 1 March	Covid-19 8 April
Death toll	50 million Higher among younger people, significant fall in workforce	774	2,996	82,220 Higher among older people, likely limited fall in workforce
Containment measures	Social distancing; vary across jurisdictions	Social distancing in China and Hong Kong SAR	Wuhan and Lombardy lockdowns	Global lockdown
Financial amplification	Little	Little	Some market sell-off	Sharp tightening in financial conditions
Real amplification	Little	Little	Supply chain disruptions	Supply chain disruptions; sudden stop in demand
Context	WWI; high share of manufacturing sector in GDP in advanced economies	Chinese growth accelerating	Highly globalised economies and integrated cross-border supply chains; high share of services sector in GDP in advanced economies; high leverage in parts of real sector	

Recent studies on the economic impact of Covid-19 face the inevitable challenge of dealing with rapidly changing circumstances.

Earlier estimates have been overtaken by events, as large-scale stringent social distancing policies were introduced and the pandemic spread. McKibbin and Fernando (2020) is one of the earliest systematic studies of potential economic cost of Covid-19.

Released at a time when a pandemic did not yet appear to be an imminent threat, roughly half of the scenarios assume the epidemic would be contained within China, leading to 0.3–2.2% loss in terms of global GDP.

In pandemic scenarios, where fatality reaches 3% and risk premia spike globally, the expected loss goes up to 11%.

UNCTAD (2020) highlights the supply chain disruptions as a result of containment measures in China, noting that 20% of global trade in manufacturing intermediate goods originates there.

They expect the European Union, the US, Japan, Korea and Taiwan to be most affected by supply disruptions.

Meanwhile, an OECD early estimate – released shortly before the pandemic started to spread in the US – suggests a 1.5% loss in terms of global GDP in a pandemic scenario.

To read more:
https://www.bis.org/publ/bisbull07.pdf

Number 2

A time for bold action

John C Williams, President and Chief Executive Officer of the Federal Reserve Bank of New York, at the Economic Club of New York.

Introduction

Thank you for the kind introduction. Hello, from my apartment in Manhattan. It's a pleasure to be able to join you today, even under these extraordinary circumstances.

I hope that wherever you are watching, you and your loved ones are safe and well.

The outbreak of the coronavirus and the global pandemic have created an unprecedented situation.

Today, I want to talk about what that means for the economy and financial markets, and how the Federal Reserve Bank of New York, and the Federal Reserve System as a whole, are responding to the challenges before us.

My colleagues and I are dedicated to doing everything within our power to support the functioning of financial markets and help put the economy on a strong footing once this crisis is behind us.

Before I continue, let me give the Fed disclaimer that the views I express are mine alone and do not necessarily reflect those of the Federal Open Market Committee or anyone else in the Federal Reserve System.

The coronavirus pandemic has created circumstances we have never experienced before in our lifetimes.

There's hardly a community in the world that remains unaffected.

I want to emphasize that this is first and foremost a public health crisis, and a human tragedy.

It's our doctors, nurses, and healthcare professionals who are on the front lines, fighting this disease and caring for those who are suffering. We owe them a great debt of gratitude.

My sincere thanks is also with the grocery store workers, those in law enforcement and transportation, and everyone who continues to carry out essential work each day.

The Scale of the Challenge

The necessary actions taken to slow and contain the spread of the coronavirus are not only changing how we live our lives, but are also having a profound effect on the economy and financial markets, both here and abroad.

Although many people have drawn comparisons with the financial crisis of 2008, the current turmoil is fundamentally different from recessions of the past.

The challenges before us do not stem from vulnerabilities at banks or the bursting of a bubble—I can only liken them to a natural disaster of global proportions.

If we look back to February, the American economy was strong, with unemployment at historical lows. But, now, social distancing and other restrictions imposed in response to the pandemic are causing severe, rapid declines in jobs and income.

Unprecedented numbers have filed for unemployment insurance in the past several weeks alone, and we know that more economic pain is still to come.

The reality is that the full scale of the economic consequences is still unknown.

The economic distress and the extraordinary uncertainty about the future course of the pandemic have set off a tidal wave of flows of money away from riskier investments to the safety of cash.

This sudden shift led to an evaporation of liquidity and breakdowns in the functioning of key financial markets.

This includes the market for U.S. Treasury securities, the cornerstone of the global financial system.

These developments, if left unchecked, threaten to starve our economy of the credit that it badly needs during this difficult time.

The Response

Last month, as the risks posed by the coronavirus became increasingly apparent, the Federal Reserve took swift and decisive action to support the economy and stabilize financial markets.

In two unscheduled meetings in the first half of March, the Federal Open Market Committee (FOMC) quickly brought the target range for the federal funds rate to near zero.

The FOMC also signaled that it expects to keep interest rates at this level until it is confident that the economy has weathered recent events and is on track to achieve the Fed's maximum employment and price stability goals.

These monetary policy actions serve two purposes.

First, low interest rates make it easier for households and businesses to meet their borrowing needs during this time of economic stress.

Second, they foster broader financial conditions that will help promote the rebound in spending and investment needed to return the economy to full strength.

To read more:
https://www.bis.org/review/r200417a.pdf

Number 3

Learning the value of resilience and technology: the global financial system after Covid-19

Benoît Cœuré, Head of the Bank for International Settlements Innovation Hub, at the Reinventing Bretton Woods Committee - Chamber of Digital Commerce webinar on "The world economy transformed".

Thank you for inviting me to speak at this webinar. I will not venture to describe the world after Covid-19. I don't know how this crisis will unfold nor when it will end. The shockwaves it sends across the global economy are just starting to be felt in the emerging and developing world - and they will spill back to us.

I would only like to suggest that two themes will shape the conversation on the "day after Covid-19": resilience and technology. Let me elaborate on what it means for international finance.

1. The value of resilience in international finance

The global financial system has withstood the Covid-19 shock better than the Great Financial Crisis. This success owes much to central banks bold action. With hindsight, it also owes a lot to action taken by regulators in the decade after the G20 Pittsburgh Summit.

Spurred by regulators, banks have built capital and liquidity buffers, improved risk management practices and internalised the social cost of risk-taking.

As a result of these efforts, they were much better prepared to cope with a major shock in 2020 than they were in 2008. They can use buffers which were simply not there at the time.

But despite progress made by macro prudential policy, we have been less good at making the global financial system more resilient as an interconnected system. We knew it before Covid-19 and the crisis has confirmed it.

Market-based finance is a well-identified gap in our macroprudential framework. We lack instruments to curb procyclicality in non-bank lending. In recent years, asset managers and funds have filled the gap left by the retrenchment of large systemic banks.

Today, in the face of outflows, they may be forced to sell assets and amplify price adjustment.

Worse, the first weeks of the Covid-19 crisis have uncovered the fragility of the price discovery mechanism in large swathes of our capital markets. Market liquidity has deteriorated faster and more broadly than in the Great Financial Crisis - when money markets had been the most affected.

Major funding markets have been strained in advanced economies. And strains are spreading fast to emerging markets, exacerbated by their uneven access to short-term dollar funding.

As a result, in the past few weeks, not only had central banks to address aggregate demand shortage, as they traditionally do, but they had to perform laser surgery on a number of market segments to make them functional again, crossing into unchartered territory.

The jury is still out yet as to whether combined central bank and government intervention will be enough to avoid the liquidity crisis morphing into a solvency one - which would raise a host of new issues.

While it is too early to start the post-mortem, there are already lessons for central banks and regulators in the post-Covid-19 world.

Efforts to make the global financial system more resilient should not be dialled back, and if anything, they should be increased.

Flexibility embedded in rules can be fully used but the rulebook itself should be protected and public support should come with conditions, such as restrictions on dividends and bonuses.

And we should renew the impulse to improve the resilience of market-based finance.

We should complete the global financial safety net as a matter of urgency, focussing on the smallest and most vulnerable economies.

The extension of the global foreign currency swap and repo network is an important step to address dollar funding needs, but it doesn't benefit all. I see lots of merits in the proposal of a new allocation of IMF Special Drawing

Rights: by providing liquidity to all IMF members, large and small, it would "get in all the cracks" of the global financial system.

2. The value of technology

The crisis has exposed the value of technologies which enable the economy to operate at arm's length and partially overcome social distancing.

Such drastic changes in work and consumption patterns, such as the dramatic shift to online shopping, will have a lasting impact on economic relationships.

The payment industry immediately comes to mind. Payments have been at the forefront of technological change recently. A rapid shift towards digital payments can improve cost, transparency and convenience for billions of consumers.

International cooperation is needed to support technological capacity in developing economies, ensure interoperability between national systems, enhance cross-border payments and remittances, and support financial inclusion - in short, to avoid spatial and social fragmentation.

The Financial Stability Board (FSB) and Committee on Payments and Market Infrastructures (CPMI) action plan on cross-border payments, which was released last week, comes timely, as well as the FSB consultative report on the regulatory implications of stablecoins.

The current discussion on central bank digital currency also comes into sharper focus. Whether Covid-19 will accelerate the demise of cash is an open question. But already, it highlights the value of having access to diverse means of payments, and the need for any means of payments to be resilient against a broad range of threats.

Covid-19 will accelerate the digital transition beyond payments. Will customers find their way back to banking branches when lockdowns are lifted and economies restart? Will this accelerate the shift towards virtual banking?

In the next months and years, the BIS Innovation Hub will remain busy scanning technological trends in finance and their consequences for central banks and financial regulators, based on practical projects.

Issues such as tokenisation, open banking, and using technology to support regulatory and supervisory compliance ("regtech" and "suptech") are high on our agenda.

Let me conclude by coming back to today's urgency.

Technology can help mitigate the economic and social impact of the Covid-19 crisis.

The debate is raging on how technology can help track the virus spread, enforce quarantines and administer remote consultations - and on which safeguards are needed to protect privacy.

Technology can also help mitigate the economic cost of lockdowns and avoid irreversible damage to the social fabric.

The most vulnerable in our societies are less likely to be reached by traditional support measures.

This is particularly the case in economies where direct tax infrastructures are less developed and the informal economy is pervasive.

Digital payments can enable governments to provide emergency support to households and small businesses affected by the virus. They can help "pump the rescue funds down the last mile".

Jurisdictions which have established retail payment and identity rails are already leveraging them to enhance their crisis response. As noted by the World Bank, the ID-linked basic account in Chile, Cuenta Rut, will allow 2 million vulnerable Chileans to benefit from Covid-related support already this month.

International coordination is key, for example to keep remittances flowing, as those normally sending them are disproportionately affected by the crisis.

For those jurisdictions which haven't established digital infrastructures, it is not too late to do so. Recent guidance by the CPMI and World Bank helps them design the right strategies to advance financial inclusion through innovation in payments.

Learning the right lessons from this crisis is not enough - there is still time to act. Thank you.

Number 4

Bumper "Patch Tuesday" releases from Microsoft

Amongst the 113 security updates in the April release from Microsoft were patches for 3 zero-day vulnerabilities. This follows a similarly large release of 115 fixes in March.

Using the latest versions of software, applications and operating systems on your devices immediately improves your security. Users should check that their device is set to update automatically.

The current COVID-19 pandemic has also seen Microsoft extend the end of life support for some Windows 10 1809 and Windows 10 1709 products. More information can be found on the Microsoft website at: https://support.microsoft.com/en-gb/help/4557164/lifecycle-changes-to-end-of-support-and-servicing-dates

The NCSC has produced some guidance to help you manage the period while you are still relying on obsolete software and platforms. You may visit: https://www.ncsc.gov.uk/collection/end-user-device-security/securing-obsolete-platforms

Number 5

NIST and OSTP Launch Effort to Improve Search Engines for COVID-19 Research

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) and the White House Office of Science and Technology Policy (OSTP) launched a joint effort to support the development of search engines for research that will help in the fight against COVID-19.

The project was developed in response to the March 16 White House Call to Action to the Tech Community on New Machine Readable COVID-19 Dataset. It can be found at: https://www.whitehouse.gov/briefings-statements/call-action-tech-community-new-machine-readable-covid-19-dataset/

"Our nation's scientific enterprise is mobilized to defeat the invisible enemy that is COVID-19," said Secretary of Commerce Wilbur Ross. "Our scientists — and the businesses and institutions that provide them with advanced digital research technologies — are to be commended for their unwavering dedication to finding a cure for this insidious disease."

"AI experts worldwide are responding to the White House's call to action, developing approaches that help scientists gain insights from thousands of articles of COVID-19 scholarly literature," said Michael Kratsios, U.S. chief technology officer.

"The TREC-COVID program expands upon these efforts by creating powerful and accurate search engines that extract knowledge from this literature, tailored to the needs of the health-care and medical research communities. We thank NIST for this valuable contribution as part of the Trump administration's whole-of-America response to the coronavirus."

In this effort, NIST will work initially with the Allen Institute for Artificial Intelligence, the National Library of Medicine, Oregon Health & Science University (OHSU), and the University of Texas Health Science Center at Houston (UT Health).

The team will apply the successful, long-running program of expert engagement and technology assessment called the Text Retrieval Conference, or TREC, to the COVID-19 Open Research Dataset (CORD-19), a resource of more than 44,000 research articles and related data about COVID-19 and the coronavirus family of viruses.

The TREC-COVID program goals include creating datasets and using an independent assessment process that will help search engine developers to evaluate and optimize their systems in meeting the needs of the research and health-care communities.

“The TREC program has provided an effective way to evaluate and advance search engine technologies since 1992, and has led directly to the powerful search capabilities and internet-based efficiencies we now often take for granted,” said Under Secretary of Commerce for Standards and Technology and NIST Director Walter G. Copan.

“We are pleased to apply this infrastructure to the challenge of working with massive amounts of data to help researchers better understand and ultimately to combat this deadly novel coronavirus and related threats.”

The team will first release a series of sample queries for the biomedical research community, developed by team members at the National Library of Medicine, OHSU and UT Health.

Registered participants in TREC-COVID will use their information retrieval and search systems to run the queries against the CORD-19 document set and return their results to NIST.

Biomedical experts will then review test results, including document relevance rankings, to assess the overall performance of the retrieval systems.

Using proven TREC protocols, NIST will score the submissions and post the scores, the retrieval results themselves, and the lists of key reference documents to the TREC-COVID website.

These “test collections” can then be used by information retrieval researchers to evaluate and enhance the performance of their own search engines.

This effort is intended to help researchers understand how search systems could best support medical researchers when available information is developing quickly, as in the current pandemic.

The Allen Institute for Artificial Intelligence has been releasing an expanded CORD-19 document set each Friday to capture the most recent articles on COVID-19 and related coronaviruses.

Later rounds of TREC-COVID will use the larger releases of CORD-19 and expanded query sets.

Participants will have one week to submit their search results, and within about a week NIST will post results, with an expected spacing of about two weeks between each new dataset round being released.

The team initially anticipates conducting five consecutive rounds of search system assessments.

Interested organizations are invited to register to participate in the TREC-COVID program on the NIST website.

NIST promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life.

Number 6

PCAOB Posts Request for Comment, Seeks Stakeholder Input on Critical Audit Matters

PCAOB
Public Company Accounting Oversight Board

The PCAOB today posted to its website a Request for Comment from the Office of Economic and Risk Analysis, which seeks input from audit firms, preparers, audit committees, investors, and other financial statement users to inform our interim analysis of the Critical Audit Matter (CAM) requirements.

We are committed to fulfilling the expectation set out for us by the U.S. Securities and Exchange Commission to complete this interim analysis before the second phase of CAM implementation begins, and we are also mindful of the many challenges related to COVID-19 that our stakeholders are dealing with at this time. To provide additional time for interested parties to share feedback with us, we extended the comment period from 30 to 60 days.

Additional information on our interim analysis and specific questions for consideration are detailed in the Request for Comment – you may visit: https://pcaobus.org/EconomicAndRiskAnalysis/pir/Documents/RFC-Interim-Analysis-CAM-Requirements.pdf

Questions for investors, analysts, and other financial statement users:

1. Have you as an investor, analyst, or other financial statement user read any auditors' reports that contain CAMs? Approximately how many? Why did you read them? Prior to CAM implementation, did you read auditors' reports?
2. What effects, if any, have investors, analysts, or other financial statement users experienced from the communication of CAMs in the auditor's report? For example, have any of the following changed as a result of CAM communications:
   - Ability to analyze companies' financial statements or make investment decisions
   - Content of analyst reports or internal buy/sell/hold recommendations
   - Interactions with management, such as developing new or better-informed questions
   - Understanding of disclosures made by company management (e.g., in MD&A)
   - Understanding of auditors' work
   - Proxy voting decisions, including ratification of the audit committee's choice of external auditor

   Please describe how CAM communications contributed to the changes and, if applicable, whether you anticipate additional changes in the future.
3. If you are an investor, analyst, or other financial statement user who has read CAMs for multiple public companies, did you find some CAMs to be more useful than others? If so, what were the factors that made them more useful?

Questions for preparers, audit committee members, and auditors:

4. Have preparers and audit committees experienced any changes in the financial reporting process as a consequence of CAM communications in the auditor's report? For example, has the communication of CAMs led to changes in controls or practices around financial reporting and disclosure? Did CAM communications result in any reconsideration of, or changes to, disclosures management made in company filings (e.g., notes to the financial statements, critical accounting estimates, MD&A, or risk factors)?
5. Have CAM communications had any impact on how audit committees approach their role and responsibilities?
6. Have auditors or preparers experienced any changes in a specific audit because of CAM requirements? For example, were there changes to the nature, timing, or extent of audit procedures performed on matters identified as CAMs, not because of changes in circumstances but because of CAM requirements?
7. Did CAM requirements lead to changes in communications between auditors, audit committees, or preparers? For instance, were there changes in the nature or frequency of communications during the audit process? Did audit committee members ask more or different types of questions? Was there more focus on matters that were identified as CAMs?
8. Based on your experience as a preparer or auditor, what were the most significant activities that led to CAM-related costs? First, please describe each activity, including any preparatory activities (e.g., pilots or dry-runs). Next, please estimate the total costs related to CAM requirements in hours (and external spend, if applicable) for each of those activities for each calendar year from 2017-2019 and the period January-April 2020, distinguishing, to the extent possible, between costs related to preparatory activities and costs related to recurring activities. Finally, for any activities that will be recurring, state whether you believe the costs will increase, decrease, or not change for each activity in future years.

We encourage commenters to provide data, evidence, and/or specific examples in support of their comments.

All comments should refer to Interim Analysis No. 2020-01, Critical Audit Matter Requirements, on the subject or reference line and should be submitted no later than June 15, 2020. Please note that comments will be posted to the PCAOB website.

Number 7

Statement on principles to mitigate the impact of Coronavirus/COVID-19 on the occupational pensions sector

1. The European Insurance and Occupational Pensions Authority (EIOPA) has been closely monitoring the coronavirus/COVID-19 developments in relation to the occupational pensions sector.

As long-term investors Institutions for Occupational Retirement Provision (IORPs) can play a stabilising role in current volatile markets.

2. Occupational pension systems across Europe are very diverse. The IORP II Directive sets minimum prudential rules for IORPs in the EU and, in consequence, prudential regulation varies considerably between Member States.

In addition, occupational pension arrangements depend on national social and labour law, resulting in differences in the extent to which risks are borne by members and beneficiaries, the IORP itself, sponsors and pension protection schemes.

3. Recognising this diversity, considering the current coronavirus / COVID-19 situation, and to mitigate the impact on IORPs and their members and beneficiaries, as well as to avoid pro-cyclical effects on the real economy and financial system, EIOPA expects national competent authorities (NCAs) to adhere to the following principles using a risk-based and proportionate approach.

Business continuity and operational risks

4. NCAs should ensure that IORPs prioritise the continuity of key operational activities, including outsourced ones, like the timely investment of contributions, the management and safekeeping of assets, the timely and accurate payment of retirement benefits and service continuity towards members and beneficiaries.

NCAs should allow IORPs flexibility in the collection of contributions from employers facing liquidity pressures, also in anticipation of envisaged wage support measures.

5. NCAs should expect IORPs to carefully consider and effectively manage the increased risk exposure to fraud, other criminal activity, cyber security and data protection due to the disruption of society and, in particular, staff working remotely.

6. To accommodate IORPs' focus on key operational activities, NCAs should be flexible with respect to deadlines for publication of documents and data considered less urgent given the current circumstances as well as in respect of national reporting requirements.

The timings for the provision of occupational pensions information to EIOPA are extended by two weeks for the information regarding the first quarter of 2020 and by eight weeks for the information regarding annual reporting with reference to the year-end 2019.

Liquidity position

7. NCAs should monitor the liquidity position of IORPs carefully and proportionately. IORPs may face significant liquidity pressures due to:

- delayed or missing contributions from employers and employees;
- the potential need to cover cash margin calls on derivative hedging positions;
- any moratorium on payments on loans and mortgages;
- expected declines in dividend payments on IORPs' equity holdings;
- difficulties in selling assets under current market circumstances.

Funding situation and pro-cyclicality

8. NCAs should closely monitor the impact of financial market developments on the financial position of IORPs providing defined benefit (DB) schemes and their compliance with national funding requirements.

9. In their supervisory responses, NCAs should seek to find an appropriate balance between the primary goal of safeguarding the long-term interests of members and beneficiaries and the aim of avoiding short-term pro-cyclical impacts on the real economy, most notably sponsoring employers, and the wider financial system.

Protection of members and beneficiaries

10. NCAs, where relevant in collaboration with the national legislator, should encourage flexibility to safeguard members' pension rights and, particularly in defined contribution (DC) schemes, allow plan members to choose delayed application of lump sum payments or of mandatory annuitisation.

Communication

11. NCAs should expect IORPs to communicate to sponsors, members and beneficiaries in a balanced way on the impact of the coronavirus/COVID-19 developments on the IORP's service continuity and, as the financial and economic impact of the COVID-19 starts to become clearer, on the impact on (future) retirement income of members and beneficiaries.

In particular in DC schemes, IORPs' communications should aim to discourage potential short-term decisions by plan members that may jeopardise long-term pension outcomes.

Number 8

Protecting healthcare and human rights organizations from cyberattacks

Tom Burt - Corporate Vice President, Customer Security & Trust

Microsoft

We're deeply concerned about cyberattacks impacting workers on the front lines of the COVID-19 fight.

News reports have shown recent criminal or nation-state attacks targeting Brno University Hospital in the Czech Republic, Paris' hospital system, the computer systems of Spain's hospitals, hospitals in Thailand, medical clinics in the U.S. state of Texas, a healthcare agency in the U.S. state of Illinois and even international bodies such as the World Health Organization.

Our teams at Microsoft have also detected and responded to attacks targeting the healthcare sector in many countries, and we know they are coming from criminals and multiple nation-states.

In addition, our threat intelligence teams have identified nation-state attacks against human rights organizations around the world for some time, both prior to and during the COVID-19 pandemic.

That's why, starting today, we're making our AccountGuard threat notification service available at no cost to healthcare providers on the front lines as well as human rights and humanitarian organizations around the world.

Healthcare organizations can sign up at:
https://www.microsoftaccountguard.com/healthcare/

Microsoft AccountGuard

Human rights and humanitarian organizations can sign up at:
https://www.microsoftaccountguard.com/humanrights/

Microsoft AccountGuard

Every patient deserves the best possible healthcare treatment, and we all need to thank and applaud the truly heroic work by those risking their own health to help those who are sick.

Their work is challenging enough but is being made more difficult by cyberattacks, now or in the future.

Some attacks, such as the one on Brno University Hospital, have resulted in delays in COVID-19 testing, new patients being turned away and treatments being postponed.

Others, such as the attack in Illinois, have held up access to critical COVID-19-related healthcare guidance.

Nearly all these attacks have two things in common: a person and email. An attacker will often disguise malicious content as a message from a health authority or medical equipment provider.

These emails sent to work or home inboxes seek to obtain the person's credentials and often contain documents or links that will infect a computer and spread the infection through a network, enabling attackers to control it.

In some cases, attackers could be looking for COVID-19-related intelligence, or to disrupt the provision of desperately needed care or supplies.

With today's announcement, we are seeking to notify customers when we see attacks and provide guidance to help.

Microsoft AccountGuard, which we first offered to political campaigns through our Defending Democracy Program, monitors nation-state threat actors targeting enterprise mailboxes and the personal email accounts of employees or volunteers who opt in.

This gives our threat intelligence teams a broad view of the avenues attackers typically use.

When we see such activity targeting an organization enrolled in AccountGuard, we notify them immediately so they can take steps to stop an attack or root out the attacker.

AccountGuard has previously been available to political campaigns, parties, members of the U.S. Congress and democracy-focused non-profits.

Nearly 100,000 email accounts in 29 countries are enrolled in AccountGuard and we've made 1,450 threat notifications to those participating.

Through today's announcement, we're making AccountGuard available to healthcare providers including hospitals, care facilities, clinics, labs and clinicians providing front line services as well as pharmaceutical, life sciences and medical devices companies that are researching, developing and manufacturing COVID-19-related treatments.

Our notifications will help these organizations defend against nation-state attacks, and our AccountGuard advice and training support will help them harden their defenses against all forms of cyberattacks.

AccountGuard for Healthcare will be available until the COVID-19 pandemic subsides.

In addition to making AccountGuard available to those working directly in the healthcare field, another important part of today's announcement is the availability of AccountGuard for worldwide human rights and humanitarian organizations.

Today, nearly every human rights or humanitarian organization is focused on protecting the rights of people impacted by COVID-19 whether it's supporting hospitals in conflict zones, amplifying the voices of medical professionals, helping to ensure elections are conducted safely in new ways or helping children who are out of school.

In many instances, nation-states and cyber criminals use attacks to gain intelligence on these organizations and the people who these groups protect, or to disrupt their work.

While cybersecurity threats are not new to human rights defenders, these groups have been increasingly under attack, even before the pandemic arose. In the past year, the Microsoft Threat Intelligence Center, or MSTIC, has tracked five separate nation-state activity groups that have attempted nearly nine hundred times to target or compromise hundreds of accounts belonging to employees of nine prominent human rights organizations around the world.

Protecting these organizations has never been more important.

Leading human rights and humanitarian organizations including Amnesty International, CyberPeace Institute, Freedom House, Human Rights Watch and Physicians for Human Rights have already registered for our AccountGuard threat notification service through an initial pilot.

Both AccountGuard for Healthcare and AccountGuard for Human Rights Organizations will initially be available to organizations in the 29 countries where we already offer AccountGuard, subject to review of local laws and regulations, and we will be adding new countries based on need and local law.

AccountGuard is available to organizations using Office 365 for business email and extends additional security to the personal accounts of their front line workers who use Microsoft's consumer email services such as Outlook.com and Hotmail.

Whether you're a front line worker or not, it's always important to make sure you trust the sender of an email before you open it, that you look out for misspellings or slight inaccuracies in emails that may offer clues of an untrustworthy message, and that you know you trust a URL before you click on it.

We've published more on protecting yourself from COVID-19-related phishing attacks at:
https://www.microsoft.com/security/blog/2020/03/20/protecting-against-coronavirus-themed-phishing-attacks/

Today's news is in addition to the work we've already announced to track and prevent cyberthreats targeting healthcare organizations and our announcement yesterday on providing non-profits working on the COVID-19 response with greater access to technology.

To read more:
https://blogs.microsoft.com/on-the-issues/2020/04/14/accountguard-cyberattacks-healthcare-covid-19/

Number 9

SEC Awards Over $27 Million to Whistleblower

Amounts Awarded to Whistleblowers by SEC Now Exceed $400 Million

The Securities and Exchange Commission has announced an award of more than $27 million to a whistleblower who alerted the agency to misconduct occurring, in part, overseas.

After providing the tip to the Commission, the whistleblower provided critical investigative leads that advanced the investigation and saved significant Commission resources.

“This award marks several milestones for the program,” said Jane Norberg, Chief of the SEC’s Office of the Whistleblower.

“This is the largest whistleblower award announced by the Commission this year, and the sixth largest award overall since the inception of the program.

This award also brings the total amount awarded to whistleblowers by the SEC over the $400 million mark.”

The SEC has awarded approximately $425 million to 79 individuals since issuing its first award in 2012.

All payments are made out of an investor protection fund established by Congress that is financed entirely through monetary sanctions paid to the SEC by securities law violators.

No money has been taken or withheld from harmed investors to pay whistleblower awards.

Whistleblowers may be eligible for an award when they voluntarily provide the SEC with original, timely, and credible information that leads to a successful enforcement action.

Whistleblower awards can range from 10 percent to 30 percent of the money collected when the monetary sanctions exceed $1 million.

As set forth in the Dodd-Frank Act, the SEC protects the confidentiality of whistleblowers and does not disclose information that could reveal a whistleblower's identity.

For more information about the whistleblower program and how to report a tip, visit www.sec.gov/whistleblower

Number 10

FBI Warns of Advance Fee and BEC Schemes Related to Procurement of PPE and Other Supplies During COVID-19 Pandemic

The Federal Bureau of Investigation is providing this industry alert to warn government and health care industry buyers of rapidly emerging fraud trends related to procurement of personal protective equipment (PPE), medical equipment such as ventilators, and other supplies or equipment in short supply during the current COVID-19 pandemic.

The FBI recently became aware of multiple incidents in which state government agencies, attempting to procure such equipment, wire transferred funds to fraudulent brokers and sellers in advance of receiving the items.

The brokers and sellers included both domestic and foreign entities.

In one case, an individual claimed to represent an entity with which the purchasing agency had an existing business relationship.

By the time the purchasing agencies became suspicious of the transactions, much of the funds had been transferred outside the reach of U.S. law enforcement and were unrecoverable.

The current environment, in which demand for PPE and certain medical equipment far outstrips supply, is ripe for fraudulent actors perpetrating advance fee and business email compromise (BEC) schemes, such as those described above.

In advance fee schemes related to procurement, a victim pre-pays (partially or in full) a purported seller or a broker for a good or service and then receives little or nothing in return.

BEC schemes often involve the spoofing of a legitimate known email address or use of a nearly identical email address to communicate with a victim to redirect legitimate payments to a bank account controlled by fraudsters.

A variation on BEC schemes can involve similar social engineering techniques via phone call.

Risk Factors

While pre-payment is more common in the current environment, it substantially increases the risk of a buyer being defrauded and eliminates most potential recourse. The following indicators are warning signs that an offer to sell items may not be legitimate:

- A seller or broker initiates the contact with the buyer, especially from a difficult to verify channel such as telephone or personal email.

- The seller or broker is not an entity with which the buyer has an existing business relationship, or the buyer's existing business relationships are a matter of public record.

- The seller or broker cannot clearly explain the origin of the items or how they are available given current demand.

- The potential buyer cannot verify with the product manufacturer that the seller is a legitimate distributor or vendor of the product, or otherwise verify the supply chain is legitimate.

- Unexplained urgency to transfer funds or a last minute change in previously-established wiring instructions.

Mitigation Recommendations

The FBI recommends that buyers consider the following recommendations to protect their companies or agencies:

- If the seller claims to represent an entity with an existing relationship to the buyer, verify claims through a known contact—do not contact the vendor through information provided in an email or phone communication.

- If possible, have a trusted independent party verify the items for sale are physically present and of the promised make, model, and quality, and take delivery immediately upon payment.

- If immediate delivery is impossible, route payments to a domestic escrow account to be released to the seller upon receipt of the promised items.

- Verify with the manufacturer or verified distributor that the seller is a legitimate distributor or vendor for the items being offered.

- Be skeptical of last minute changes in wiring instructions or recipient account information—do not re-route payments without independently verifying the direction came from an authorized party.

- Verify the email address used to send emails, especially when using a mobile or handheld device, by ensuring the sender's email address appears to match who it is coming from.

If you think your company or agency is the victim of a fraud scheme related to COVID-19 immediately contact the FBI's Internet Crime Complaint Center at ic3.gov.

For accurate and up-to-date information about COVID-19, you may visit:

coronavirus.gov
cdc.gov/coronavirus
usa.gov/coronavirus
fbi.gov/coronavirus
justice.gov/coronavirus

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.

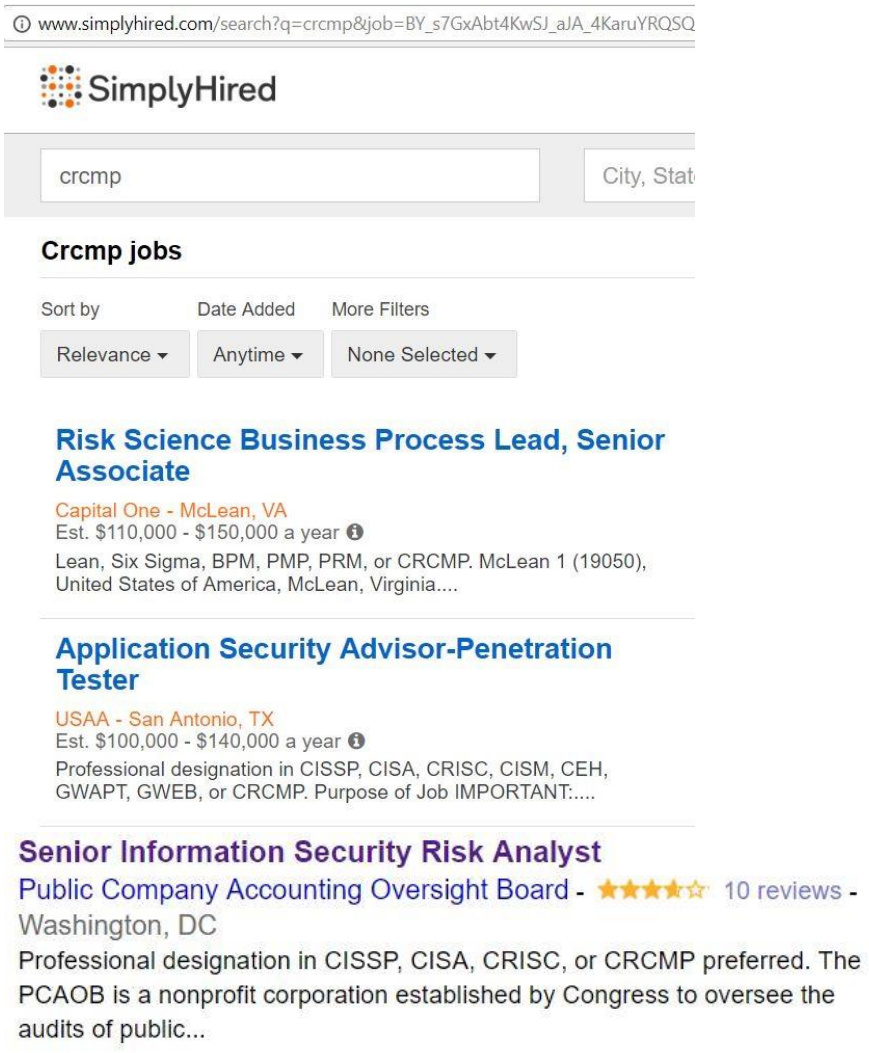
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

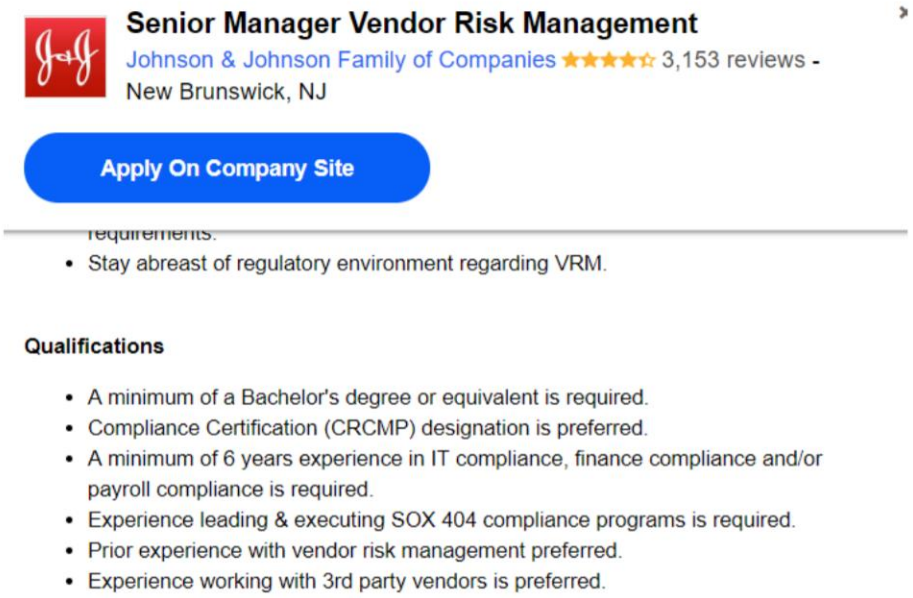
You can explore what we offer to our members:

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.

4. *IARCP Authorized Certified Trainer (IARCP-ACT) Program* - This is an additional advantage on your resume, serving as a third-party endorsement to your knowledge and experience.

Certificates are important when being considered for a promotion or other career opportunities. You give the necessary assurance that you have the knowledge and skills to accept more responsibility.

To learn more, you may visit:
https://www.risk-compliance-association.com/IARCP_ACT.html

5. *Approved Training and Certification Centers (IARCP-ATCCs)* - In response to the increasing demand for CRCMP training, the International Association of Risk and Compliance Professionals is developing a world-wide network of Approved Training and Certification Centers (IARCP-ATCCs).

This will give the opportunity to risk and compliance managers, officers, and consultants to have access to instructor led training at convenient locations that meet international standards.

ATCCs use IARCP approved course materials and have access to IARCP Authorized Certified Trainers (IARCP-ACTs).

To learn more:
https://www.risk-compliance-association.com/Approved_Centers.html