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, March 15, 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,

Disinformation on social media comes in many shapes and forms. It can manifest as a piece of fake news that is shared, a deliberately false post or a comment, a network of automated accounts pushing a specific narrative, a misleading meme, an anonymous user engaged in trolling, or a targeted advertisement with misleading content.

This is part of a new document I have just read for the second time, with title *Social Media Monitoring: A Primer, Methods, tools, and applications for monitoring the social media space,* published by the NATO Strategic Communications Centre of Excellence. We read:

Actors who produce and spread disinformation on social media use established infrastructures and exploit existing issues and polarised audiences; this gives them an advantage.

These actors tend to be agile and flexible. They use multiple techniques, engage in trial-and-error, make use of multiple platforms, and are not bound by any fixed modus operandi (although some techniques recur frequently).

The scope of disinformation is often unknown, and we often fail to see the big picture until it is too late. Disinformation spread during a specific political event may not be aimed at influencing current developments but might be designed to achieve a longer-term effect.

According to the FIRST Principles of Disinformation:

Fabrication: Disinformation often manipulates or fabricates content, such as including untrue information, attaching a manipulated picture, or sharing a doctored video.

Identity: Disinformation frequently makes use of false identities and sources, such as an anonymous or fake account.

Rhetoric: Disinformation is not necessarily false but can also make use of malign or false arguments to skew a discussion. Trolling is an example of how harsh rhetoric can be used to this end.

Symbolism: Disinformation leverages and exploits events for their symbolic and communicative value.

Technology: Disinformation exploits a technological advantage, for example, by using automated accounts to amplify their spread.

This document covers many interesting aspects. For example, we read about the intelligence cycle:

The intelligence cycle is a basic model of the analytical process used in the intelligence community to collect, process, and use information.

It is by no means the perfect model for every task, but it serves as a useful starting point for social media monitoring.

The intelligence cycle is a well-established concept that has been written about at length elsewhere. For the purposes of this paper, we will briefly highlight the most important considerations for each step of the process.

The intelligence cycle consists of five stages:
1. Direction
2. Collection

3. Processing
4. Analysis
5. Dissemination.

The intelligence cycle is a cycle for a reason—the process of establishing a direction, collecting information, analysing it, and producing meaningful outputs is a continuous one.

The results of each monitoring cycle provide feedback that drives new information needs and leads to fine-tuning for the next cycle.

The intelligence process. Source: Joint Intelligence / Joint Publication 2-0 (Joint Chiefs of Staff)

Disinformation is a hot subject, and it is becoming more important. You can read more at number 2, 3 and 6 below. Welcome to the top 10 list.

Best regards,

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

Number 1 (Page 6)

The tale of the three stabilities - price stability, financial stability and economic stability -

François Villeroy de Galhau, Governor of the Bank of France, at the Financial Stability Review Conference.

Number 2 (Page 9)

SOCIAL MEDIA MONITORING: A PRIMER

Methods, tools, and applications for monitoring the social media space, NATO Strategic Communications Centre of Excellence

Number 3 (Page 12)

RESIST, Counter-disinformation toolkit

Number 4 (Page 15)

EBA issues new supervisory reporting and disclosures framework for investment firms

Number 5 (Page 18)

U.S. Economic Outlook and Monetary Policy: An Update

Governor Lael Brainard, Federal Reserve Board of Governors, at the C. Peter McColough Series on International Economics, Council on Foreign Relations, New York, New York.

Number 6 (Page 25)

Final report, National Security Commission on Artificial Intelligence (756 pages)

Number 7 (Page 26)

BIS Working Papers No 930 - Big data and machine learning in central banking

Sebastian Doerr, Leonardo Gambacorta and Jose Maria Serena, Monetary and Economic Department, March 2021

Number 8 (Page 29)

Report to Congressional Committees

HIGH-RISK SERIES: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas

Number 9 (Page 31)

Developing Virtual Partners to Assist Military Personnel

Program seeks to develop AI technologies capable of helping humans perform complex tasks, expand skills, and reduce errors

Number 10 (Page 34)

Advice following Microsoft vulnerabilities exploitation

Urgent updates released for Exchange server vulnerabilities

Number 1

The tale of the three stabilities - price stability, financial stability and economic stability

François Villeroy de Galhau, Governor of the Bank of France, at the Financial Stability Review Conference.

It is a great pleasure for me to welcome you to the publication today of the 24th edition of the Banque de France Financial Stability Review. We have a set of very distinguished speakers.

I would like to thank them and all the contributors to the review, as well as the Banque de France's teams who helped prepare this issue, which focuses on macroprudential policy in the midst of the Covid crisis.

The past twelve months have seen some of the most dramatic events since World War II, with this unprecedented pandemic. For this reason, and given that today is about the Financial Stability Review, I will focus on the concept of stability itself.

Other sources of instability have affected the world economy in the past decade or so: the Global Financial Crisis and ensuing recession, the European Debt Crisis, or more recently rising trade tensions.

It seems that the world has become more unstable. Against this backdrop, stability is all the more important for our fellow citizens, and it has different dimensions, but I will focus mainly on three key aspects.

I will start (and it will be a surprise to no one) with price stability. I will then turn to financial stability, which is essential for the effectiveness of monetary policy (by preserving its transmission channels).

Finally, I will talk about economic stability and the way monetary policy, in combination with fiscal policy, can smooth the business cycle and foster a robust and sustainable recovery from the covid crisis.

Clearly, these different aspects are closely intertwined: monetary policy, while pursuing its primary objective of price stability, can affect financial stability; fiscal and monetary policy closely interact with each other, as do

monetary and macroprudential policy. But for the sake of clarity I will tackle each concept in turn.

I. Price stability

To achieve the ECB inflation objective, we are determined to maintain, as long as necessary, a very accommodative monetary stance. We continue to stand ready to adjust all of our instruments, as appropriate, including possibly a lowering of the DFR if needed.

And to guarantee the full transmission of this accomodative stance, we pay particular attention to ensuring that both bank and market financing conditions remain favourable for all agents (governments, firms and households).

This leads us to monitor a large set of indicators, with a multifaceted and holistic approach.

Let me add some comments about the recent increase we have seen in long-term rates, following although to a lesser extent the move in the US. This increase has different causes, and hence calls for different reactions and instruments.

First, in the euro area, the latest consumer price data have surprised on the upside, and there are some signs of an upturn in inflation expectations. This is actually good news, as Philip Lane noted last week.

That said, this rise shouldn't be overstated; it primarily reflects temporary factors rather than a persistent and significant change in the inflation path. The euro area economy is in a different situation compared with that of the US (in terms of real activity, output gap and fiscal stimulus). There is no risk of overheating in Europe.

Second, this less disinflationary environment shouldn't raise questions about our future monetary policy, and our reaction function. Let me reiterate a strong conviction about our inflation objective: it is flexible, symmetric and medium-term.

To put it clearly, these last two imperatives mean that we cannot completely ignore the past inflation shortfalls, and that in the future we should be ready to accept inflation above target for some time.

As necessary, our forward guidance could be strengthened to make this tolerance explicit.

And third, there are other elements in this tightening of financing conditions, including excessive spillovers and tensions on the term premia.

In so much as this tightening is unwarranted, we can and must react against it, starting with an active flexibility of our PEPP purchases, which we have made possible since its inception in March 2020, and enhanced last December.

To read more:
https://www.bis.org/review/r210304d.htm

Number 2

SOCIAL MEDIA MONITORING: A PRIMER

Methods, tools, and applications for monitoring the social media space, NATO Strategic Communications Centre of Excellence

For the last twenty years, the phenomenon of social media has cemented itself as the new nexus of social interaction. With billions of users across the world, hundreds of online platforms, and a myriad of digital technologies at its backbone, social media is fundamentally reshaping our understanding of the global information environment.

Today, social media is essential infrastructure for personal conversation, public debate, and commercial communication.

While social media provides many opportunities for unprecedented information sharing, the rapid adoption of limitless communication technologies with instant amplification and global reach has also created significant vulnerabilities.

Social media have, in many cases, become a conduit for unsubstantiated information, such as rumours, hoaxes, and conspiracy theories.

Even more worrisome from a national security perspective, hostile actors are deliberately exploiting social media to spread disinformation and to conduct information influence activities with the intent of deceiving and misleading audiences to achieve their strategic aims.

Contemporary conflicts, especially those that fall within the hybrid spectrum, increasingly play out over social media, and actors such as Russia, China, Iran, and Saudi Arabia have recently expanded their efforts to manipulate the social media space.

Malicious use of social media poses a clear security challenge. The opportunities provided by new digital technologies are exploited to undermine trust in democratic institutions and legitimate news sources, to distort public discourse and opinion formation, and to influence elections and short-circuit decision-making processes.

For this reason, it is important for a wide array of stakeholders to understand what is happening on social media.

Effectively listening to conversations online and monitoring and analysing social media content is crucial for both public and private sector actors, as well as for military organisations.

This, however, is easier said than done. The complex social and technical infrastructure of the online environment makes both seeing the big picture and identifying specific pieces of information challenging.

The speed at which information flows between social media users, and the ever-changing types of data generated further complicate the picture.

The deceptive nature of disinformation and information influence activities also make detection and attribution difficult.

It has quickly become clear that attaining perfect situational awareness of the online information environment is a tall order.

Still, while much of today's information environment is essentially characterised by perpetual chaos, it is possible to study and understand it, albeit momentarily.

Even snapshots of a bigger picture are critical for operating successfully in this space.

The importance of understanding what is happening on social media has prompted the development of a wide range of tools to monitor, measure, and analyse metrics and content.

Oftentimes these tools are developed with either a commercial objective—monitoring brand engagement or customer discourse—or with a scholarly mindset— to understand wider patterns and trends.

However, these tools can also be leveraged to gain insights regarding disinformation and other security concerns.

To read more:
https://www.stratcomcoe.org/social-media-monitoring-primer

Types of social media:

Social networks | Media-sharing networks | Social messaging platforms | Blogging networks | Discussion boards | Review networks

Information influence activities

"Information influence activities are activities conducted by foreign powers to influence the perceptions, behaviour, and decisions of target groups to the benefit of foreign powers."

Pamment et al. (2018) Countering Information Influence Activities: The Start of the Art, MSB

"NATO views **disinformation** as the deliberate creation and dissemination of false and/or manipulated information with the intent to deceive and/or mislead. Disinformation seeks to deepen divisions within and between Allied nations, and to undermine people's confidence in elected governments."

NATO (2020) NATO's approach to countering disinformation: A focus on COVID-19

Number 3

RESIST, Counter-disinformation toolkit

RESIST Disinformation: a toolkit
The purpose of this toolkit is to help you prevent the spread of disinformation. It will enable you to develop a response when disinformation affects your organisation's ability to do its job, the people who depend on your services, or represents a threat to the general public.

What is disinformation?
Disinformation is the deliberate creation and/or sharing of false information with the intention to deceive and mislead audiences. The inadvertent sharing of false information is referred to as misinformation.

Who is this toolkit for?
Government and public sector communications professionals, as well as policy officers, senior managers and special advisers.

Recognise disinformation

Disinformation is about influence. The people who spread it do not want members of the public to make informed, reasonable choices. They try to achieve a goal by deliberately shortcutting normal decision-making processes.

The basic techniques are simple – we call them the FIRST principles of disinformation:

• Fabrication manipulates content: for example, a forged document or Photoshopped image;

• Identity disguises or falsely ascribes a source: for example, a fake social media account or an imposter;

• Rhetoric makes use of malign or false arguments: for example, trolls agitating commenters on a chat forum;

• Symbolism exploits events for their communicative value: for example terrorist attacks; and

• Technology exploits a technological advantage: for example bots automatically amplifying messages.

These FIRST principles of disinformation are often combined to create an impact.

FIRST principles, combined

1. Look for a social issue that is sensitive or holds symbolic value.

2. Create two or more social media accounts under false identities.

3. Manipulate content to provoke a response within the sensitive issue.

4. Release the content through one account.

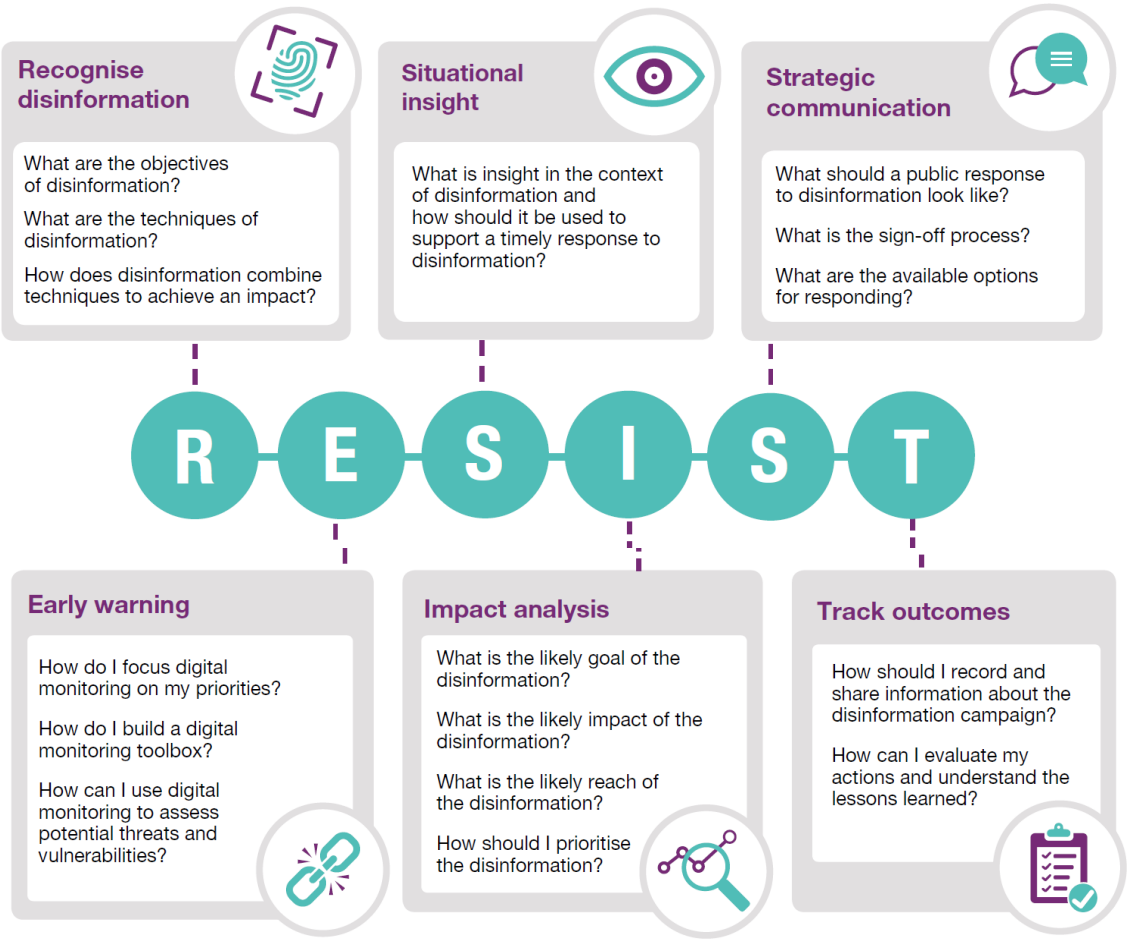
5. Criticise it through others.

6. Use bots to amplify the manipulated content to opposing networks.

7. Use memes and trolling to give the impression of a heated public debate.

Potential impact: Undermine confidence in government or between social groups; contribute to political polarisation; earn money through clicks; go viral and reach mainstream news.

SATIRE AND PARODY (R, S) Ridiculing and humouring of individuals, narratives or opinions to undermine their legitimacy.	A public figure is ridiculed using memes where non-factual opinions are ascribed to the public figure.
SHILLING (I) To give credibility to a person or a message without disclosing intentions or relationships.	An actor endorses certain content while appearing to be neutral but is in fact a dedicated propagandist.
SOCKPUPPETS (I, R, T) Use of digital technology to disguise identity, to play both sides of a debate.	A user creates two or more social media accounts under opposing identities i.e. one pro-fox hunting, one against, with the aim of playing the identities against one another.
SPIRAL OF SILENCE (S) The decrease in audibility of deviant opinions due to non-conforming beliefs.	A person with non-conforming minority beliefs is less willing to share his or her opinions.
TROLLING (I, R, S) Deliberate commenting on internet forums to provoke and engage other users in argument.	Social media users deliberately post provocative comments to create emotional outrage in other users.
WOOZLE EFFECT (R) Self-perpetuating evidence by citation.	A false source is cited repeatedly to the point where it is believed to be true because of its repeated citation.



To learn more:
https://gcs.civilservice.gov.uk/publications/resist-counter-disinformation-toolkit/

Number 4

EBA issues new supervisory reporting and disclosures framework for investment firms

- The new reporting and disclosures framework reflects the prudential requirements for investment firms as defined in the Investment Firms Regulation (IFR).

- The final draft ITS take into account the different classes of investments firms to ensure requirements are proportionate to the nature, size and complexity of investment firms.

- Consistency and integration between both reporting and disclosures will facilitate the implementation of these new requirements.

The European Banking Authority (EBA) published today its final draft Implementing Technical Standards (ITS) on the supervisory reporting and disclosures of investment firms.

These final draft ITS, which are part of the phase 1 mandates of the EBA roadmap on investment firms, will ensure a proportionate implementation of the new prudential framework for investment firms taking into account the different activities, sizes and complexity of investments firms.
You may visit:
https://www.eba.europa.eu/sites/default/documents/files/document_library/Regulation%20and%20Policy/Investment%20firms/884436/EBA%20Roadmap%20on%20Investment%20Firms.pdf

Figure 1: Thematic areas covered by the EBA mandates

The implementing technical standards included in this package set out the main aspects of the new reporting framework in relation to the calculation of own funds, levels of minimum capital, concentration risk, liquidity requirements and the level of activity in respect of small and non-interconnected investment firms.

The ITS propose a different set of templates to cover small and non-interconnected investment firms, and to include information that is proportionate to their size and complexity.

In addition, the ITS includes a standardised set of templates for the disclosures of own funds. The EBA is issuing a single set of standards with integrated Pillar 3 disclosures and supervisory reporting requirements and standardised formats and definitions with a view to improving consistency between reporting and disclosures requirements, which will facilitate compliance with both requirements.

Implementation and remittance date
The disclosure requirements will be applicable from 26 June 2021.
The first reporting reference date is September 2021 (for quarterly reports) and December 2021 (for annual reports).

DOCUMENTS

- Final Draft ITS on Reporting and disclosures for investment firms
- Annex I - Reporting for Class 2 investment firms
- Annex II - Reporting for Class 2 investment firms
- Annex III - Reporting Class 3 investment firms
- Annex IV - Reporting for Class 3 investment firms
- Annex V - DPM and validation rules
- Annex VI - Disclosure of own funds
- Annex VII - Disclosure of own funds
- Annex VIII - Reporting on group capital test
- Annex IX - Reporting on group capital test

LINKS

- Reporting framework 3.1
- Regulatory Technical Standards on prudential requirements for investment firms
- Technical Standards on reporting and disclosures requirements for investment firms
- Investment firms
- Supervisory reporting
- Transparency and Pillar 3

Legal basis and background

The EBA has developed these draft ITS according to Article 54(3) and Article 49(2) of the IFR - (EU) 2019/2033 - which mandates the EBA to develop a reporting framework and a disclosure requirements for investment firms.

The Investment Firms Prudential Package consists of the Directive (EU) 2019/2034 and the Regulation (EU) 2019/2033, which were published in the Official Journal on 5 December 2019 and establish a new prudential framework for investment firms authorised under MIFID.

To read more:
https://www.eba.europa.eu/eba-issues-new-supervisory-reporting-and-disclosures-framework-investment-firms

Number 5

U.S. Economic Outlook and Monetary Policy: An Update

Governor Lael Brainard, Federal Reserve Board of Governors, at the C. Peter McColough Series on International Economics, Council on Foreign Relations, New York, New York.

It has been one year since the first wave of the COVID-19 pandemic hit our shores—a year marked by heartbreak and hardship.

We are all looking forward to a brighter time ahead, when vaccinations are widespread, the recovery is broad based and inclusive, and services, schools, sports, and social life are in person.

The expected path of the U.S. economy has strengthened with the prospect of widespread vaccinations and additional fiscal stimulus, but risks remain, and we are currently far from our goals.

Current Situation

After a dark winter with elevated case counts and setbacks on service-sector jobs, case counts have come down and spending is picking up. Economic forecasts for growth during the first quarter have been significantly upgraded in response to the better-than-expected data.

January data for household spending overall came in strong—confirming that the renewal of fiscal support at the end of the year provided a much needed boost to household incomes and spending at the turn of the year.

The income support provided by fiscal authorities to hard-hit workers, households, businesses, and states and localities, as well as the actions of the Federal Reserve to promote orderly functioning in financial markets and low borrowing costs for households and businesses, have been providing vital support for the economy.

In recent weeks, vaccinations have been increasing, while weekly cases, hospitalizations, and deaths have decreased. The seven-day moving average of daily COVID deaths, which peaked in mid-January, declined about 35 percent during the month of February, although sadly it is still at high

levels. As of yesterday, nearly 77 million vaccination doses had been administered.

While the progress on vaccinations is promising, jobs are currently down by 10 million relative to pre-pandemic levels. Improvements in the labor market stalled late last year after rebounding partway in the summer and fall of 2020.

When we take into consideration the more than 4 million workers who have left the labor force since the pandemic started, as well as misclassification errors, the unemployment rate is close to 10 percent currently—much higher than the headline unemployment rate of 6.3 percent.

Labor force participation by prime-age workers stands lower now, on net, than it did in June after it had bounced back partway from the decline in April.

The decline in labor force participation relative to last June is largely a result of lower participation by prime-age women, which, in turn, partly reflects the increase in caregiving work at home with the move to remote schooling and the shutdown of daycares due to COVID.

On average, over the period from November 2020 to January 2021, the fraction of prime-age women with children aged 6 to 17 who were out of the labor force for caregiving had increased by 2.4 percentage points from a year earlier, while for men the fraction had increased by about 0.6 percentage point.

If not soon reversed, the decline in the participation rate for prime-age women could have scarring effects, with longer-term implications for household incomes and potential growth.6

Roughly 90 percent of the shortfall in private payroll employment relative to the pre-COVID level is concentrated in service-providing industries, with half of these service job losses in leisure and hospitality.

The concentration of job losses in services has had a disproportionate effect on the lowest-wage workers. Workers in the lowest-wage quartile face an extremely elevated rate of unemployment of around 23 percent.

The advent of widespread vaccinations should revive in-person schooling and childcare along with demand for the in-person services that employ a significant fraction of the lower-wage workforce.

Realized inflation remains low, although inflation expectations appear to have moved closer to our 2 percent longer-run target.

Both core and headline measures of 12-month personal consumption expenditures (PCE) inflation were 1.5 percent in January, well below our longer-run 2 percent inflation goal.

Longer-term inflation expectations appear to have moved up in recent months, consistent with the Federal Open Market Committee's (FOMC) new commitment to achieving inflation that averages 2 percent over time.

Market-based indicators of inflation expectations increased over recent months, with Treasury Inflation-Protected Securities-based measures of inflation compensation over the next 5 years and 10 years rising about 40 and 30 basis points, respectively, since the end of last year.

Some survey measures of inflation expectations have also moved up in recent months, although, on balance, they have only moved up toward their pre-COVID levels.

In many foreign countries, growth moderated at the end of 2020, as a spike in COVID hospitalizations and deaths led to tighter public health restrictions in many economies.

Retail sales and measures of services activity weakened even as manufacturing and exports remained more resilient. Foreign activity should strengthen later this year as vaccinations rise, COVID case counts decline, and social distancing eases.

It should also be aided by some rundown in the stock of excess savings, continued fiscal and monetary support, and strong U.S. demand.

The turnaround in growth in each country will hinge on success in controlling the virus and limiting economic scarring from the past year's downturn, as well as on available policy space, and underlying macroeconomic vulnerabilities.

Outlook

So, what do these developments suggest for the U.S. outlook? Increasing vaccinations, along with enacted and expected fiscal measures and accommodative monetary policy, point to a strong modal outlook for 2021, although considerable uncertainty remains.

It is widely expected that we will continue to make progress controlling the virus, reducing the need for social distancing, but variants of the virus, slow take-up of vaccinations, or both could slow progress.

Additional fiscal support is likely to provide a significant boost to spending when vaccinations are sufficiently widespread to support a full reopening of in-person services. Various measures of financial conditions are broadly accommodative relative to historical levels and should remain so.

The labor market should strengthen, perhaps significantly, as the virus recedes, social distancing comes to an end, and the service sector springs back to life.

Inflation is likely to temporarily rise above 2 percent on a 12-month basis when the low March and April price readings from last year fall out of our preferred 12-month PCE measure.

Transitory inflationary pressures are possible if there is a surge of demand that outstrips supply in certain sectors when the economy opens up fully.

The size of such a surge in demand will depend in part on the effects of additional fiscal stimulus, along with any spend-down of accumulated savings, which are uncertain.

But a surge in demand and any inflationary bottlenecks would likely be transitory, as fiscal tailwinds to growth early this year are likely to transition to headwinds sometime thereafter.

A burst of transitory inflation seems more probable than a durable shift above target in the inflation trend and an unmooring of inflation expectations to the upside.

When considering the inflation outlook, it is important to remember that inflation has averaged slightly below 2 percent for over a quarter-century.

In the nine years since the FOMC's announcement of a 2 percent inflation objective, 12-month PCE inflation has averaged under 1-1/2 percent.

Readings of 12-month inflation have been below 2 percent in 95 of those 109 months.

According to recent research, statistical models estimate that underlying core PCE inflation ranges from one- to four-tenths of 1 percentage point below our 2 percent longer-run target.

Recall that at the end of 2019, with unemployment at a multidecade low and after the addition of almost 1-1/2 million workers to the labor force during the previous year, PCE inflation was 1.6 percent for the year.

Monetary Policy

With that outlook in mind, let me turn to monetary policy. After an extensive review, the FOMC revised its monetary policy framework to reflect important changes in economic relationships characterized by a low equilibrium interest rate, inflation persistently below target, and low sensitivity of inflation to resource utilization.

The new framework calls for monetary policy to seek to eliminate shortfalls of employment from its maximum level, in contrast to the previous approach that called for policy to minimize deviations when employment is too high as well as too low.

It emphasizes that maximum employment is a broad-based and inclusive goal assessed by a wide range of indicators.

In addition, in order to keep longer-term inflation expectations well anchored at our 2 percent goal, monetary policy will seek to achieve inflation that averages 2 percent over time.

Consequently, following periods when inflation has been running persistently below 2 percent, appropriate monetary policy will likely aim to achieve inflation moderately above 2 percent for some time.

These changes mean that we will not tighten monetary policy solely in response to a strong labor market. The long-standing presumption that accommodation should be reduced preemptively when the unemployment rate nears estimates of the neutral rate in anticipation of high inflation that is unlikely to materialize risks an unwarranted loss of opportunity for many of the most economically vulnerable Americans.

It may curtail progress for racial and ethnic groups that have faced systemic challenges in the labor force. Instead, the shortfalls approach will enable the labor market to continue to improve absent clear indications of high inflationary pressures or an unmooring of inflation expectations to the upside.

The FOMC has set out forward guidance on the policy rate and asset purchases that implements the new framework. The guidance indicates an expectation that it will be appropriate to maintain the current target range of the federal funds rate until labor market conditions have reached levels

consistent with the Committee's assessments of maximum employment and inflation has risen to 2 percent and is on track to moderately exceed 2 percent for some time.

Even after economic conditions warrant liftoff, changes in the policy rate are likely to be only gradual, as the forward guidance notes that monetary policy will remain accommodative in order to achieve inflation moderately above 2 percent for some time so that inflation averages 2 percent over time.

In addition, asset purchases are expected to continue at least at their current pace until substantial further progress has been made toward our goals.

In assessing substantial further progress, I will be looking for realized progress toward both our employment and inflation goals.

I will be looking for indicators that show the progress on employment is broad based and inclusive rather than focusing solely on the aggregate headline unemployment rate, especially in light of the significant decline in labor force participation since the spread of COVID and the elevated unemployment rate for workers in the lowest-wage quartile and other disproportionately affected groups.

Likewise, while I will carefully monitor inflation expectations, it will be important to achieve a sustained improvement in actual inflation to meet our average inflation goal.

The past decade of underperformance on our inflation target highlights that reaching 2 percent inflation will require patience, and we have pledged to hold the policy rate in its current range until not only has inflation risen to 2 percent but it is also on track to moderately exceed 2 percent for some time.

Of course, we will be vigilant in parsing the data. Given the path of inflation to date, our framework calls for inflation moderately above 2 percent for some time.

If, in the future, inflation rises immoderately or persistently above target, and there is evidence that longer-term inflation expectations are moving above our longer-run goal, I would not hesitate to act and believe we have the tools to carefully guide inflation down to target.

Today the economy remains far from our goals in terms of both employment and inflation, and it will take some time to achieve substantial further progress. Jobs are still 10 million below the pre-COVID level, and

inflation has been running below 2 percent for years. We will need to be patient to achieve the outcomes set out in our guidance.

Number 6

Final report, National Security Commission on Artificial Intelligence (756 pages)

The report emphasized that with the increased use of AI by foreign powers to spread disinformation online and launch cyberattacks, the U.S. is falling behind in guarding against such threats.

The report:
https://assets.foleon.com/eu-west-2/uploads-7e3kk3/48187/nscai_full_report_digital.04d6b124173c.pdf

Number 7

BIS Working Papers No 930 - Big data and machine learning in central banking

Sebastian Doerr, Leonardo Gambacorta and Jose Maria Serena,
Monetary and Economic Department, March 2021

Abstract

This paper reviews the use of big data and machine learning in central banking, leveraging on a recent survey conducted among the members of the Irving Fischer Committee (IFC).

The majority of central banks discuss the topic of big data formally within their institution. Big data is used with machine learning applications in a variety of areas, including research, monetary policy and financial stability.

Central banks also report using big data for supervision and regulation (suptech and regtech applications).

Data quality, sampling and representativeness are major challenges for central banks, and so is legal uncertainty around data privacy and confidentiality.

Several institutions report constraints in setting up an adequate IT infrastructure and in developing the necessary human capital. Cooperation among public authorities could improve central banks' ability to collect, store and analyse big data.

Introduction

The world is changing and so is the way it is measured. For decades, policymakers and the private sector have relied on data released by official statistical institutions to assess the state of the economy.

Collecting these data require substantial effort and publication often happens with a lag of several months or even years.

However, the last years have seen explosive growth in the amount of readily available data.

New models of data collection and dissemination enable the analysis of vast troves of data in real time. We now live in the "age of big data".

One major factor in this development is the advent of the information age, and especially the smart phone and cloud computing: individuals and companies produce unprecedented amounts of data that are stored for future used in servers of technology companies.

For example, billions of Google searches every day reveal what people want to buy or where they want to go for dinner. Social media posts allow market participants to track the spread of information in social networks.

Companies record every step of their production or selling process, and electronic payment transactions and e-commerce create a digital footprint. An additional catalyst in the creation of big data, especially financial data, has been the Great Financial Crisis (GFC) of 2007-09.

The GFC laid bare the necessity of more disaggregated data: a relatively small but interconnected bank such as Lehman Brothers could bring down the financial system because it was highly interconnected.

The regulation and reporting requirements set up after the GFC have increased the data reported to central banks and supervisory authorities – and further work to enhance central bank statistics is in progress (Buch (2019)).

The advent of big data coincides with a quantum leap in technology and software used to analyse it: artificial intelligence (AI) is the topic du jour and enables researchers to find meaningful patterns in large quantities of data.

For example, natural language processing (NLP) techniques convert unstructured text into structured data that machine-learning tools can analyse to uncover hidden connections.

Network analysis can help to visualise relations in these high-dimensional data.

For the first time in history, it is possible to produce a real-time picture of economic indicators such as consumer spending, business sentiment or people's movements.

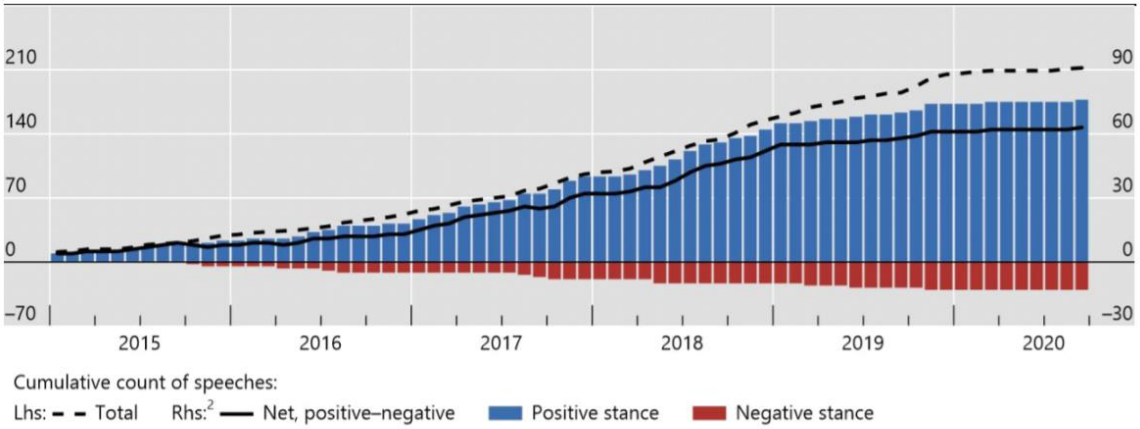
These developments have spurred central banks' interest in big data.

Rising interest is reflected in the number of central bank speeches that mention big data and do so in an increasingly positive light (Graph 1). And yet, big data and machine learning pose challenges – some of them more general, others specific to central banks and supervisory authorities.

Central banks' interest in big data is mounting[1]

Number of speeches

Graph 1



[1] Search on keyword "big data". [2] The classification is based on the authors' judgment. The score takes a value of –1 if the speech stance was clearly negative. It takes a value of +1 if the speech stance was clearly positive or a project/pilot using big data has been conducted. Other speeches (not displayed) have been classified as neutral.

Sources: Central bankers' speeches; authors' calculations.

This paper reviews the use of big data and machine learning in the central bank community, leveraging on a survey conducted in 2020 among the members of the Irving Fischer Committee (IFC).

The survey contains responses from 52 respondents from all regions and examines how central banks define and use big data, as well as which opportunities and challenges they see.

To read more: https://www.bis.org/publ/work930.pdf

Number 8

Report to Congressional Committees

HIGH-RISK SERIES: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas

Overall ratings in 2021 for 20 of GAO's 2019 high-risk areas remain unchanged, and five regressed.

Seven areas improved, one to the point of removal from the High-Risk List.

Two new areas are being added, bringing our 2021 High-Risk List to 36 areas.

Where there has been improvement in high-risk areas, congressional actions, in addition to those by executive agencies, have been critical in spurring progress.

GAO is removing Department of Defense (DOD) Support Infrastructure Management from the High-Risk List.

Among other things, DOD has more efficiently utilized military installation space; reduced its infrastructure footprint and use of leases, reportedly saving millions of dollars; and improved its use of installation agreements, reducing base support costs.

GAO is narrowing the scope of three high-risk areas by removing segments of the areas due to progress that has been made.

The affected areas are:

(1) Federal Real Property (Costly Leasing) because the General Services Administration has reduced its reliance on costly leases and improved monitoring efforts;

(2) DOD Contract Management (Acquisition Workforce) because DOD has significantly rebuilt its acquisition workforce; and

(3) Management of Federal Oil and Gas Resources (Offshore Oil and Gas Oversight) because the Department of the Interior's Bureau of Safety and Environmental Enforcement has implemented reforms improving offshore oil and gas oversight.

National Efforts to Prevent, Respond to, and Recover from Drug Misuse is being added to the High-Risk List. National rates of drug misuse have been increasing, and drug misuse has resulted in significant loss of life and harmful effects to society and the economy.

GAO identified several challenges in the federal government's response, such as a need for greater leadership and coordination of the national effort, strategic guidance that fulfills all statutory requirements, and more effective implementation and monitoring.

Emergency Loans for Small Businesses also is being added. The Small Business Administration has provided hundreds of billions of dollars' worth of loans and advances to help small businesses recover from adverse economic impacts created by COVID-19.

While loans have greatly aided many small businesses, evidence of fraud and significant program integrity risks need much greater oversight and management attention.

Nine existing high-risk areas also need more focused attention (see table).

2021 High-Risk List Areas Requiring Significant Attention

High-risk areas that regressed since 2019	High-risk areas that need additional attention
USPS Financial Viability	IT Acquisitions and Operations
Decennial Census	Limiting the Federal Government's Fiscal Exposure by Better Managing Climate Change Risks
Ensuring the Cybersecurity of the Nation	U.S. Government's Environmental Liability
Strategic Human Capital Management	Improving Federal Oversight of Food Safety
EPA's Process for Assessing and Controlling Toxic Chemicals	

To read more: https://www.gao.gov/reports/GAO-21-119SP/

Number 9

Developing Virtual Partners to Assist Military Personnel

Program seeks to develop AI technologies capable of helping humans perform complex tasks, expand skills, and reduce errors

Increasing worker knowledge, productivity, and efficiency has been a seemingly never ending quest for the military as well as commercial companies.

Today, military personnel are expected to perform a growing number of complex tasks while interacting with increasingly sophisticated machines and platforms.

Artificial intelligence (AI) enabled assistants have the potential to aid users as they work to expand their skillsets and increase their productivity.

However, the virtual assistants of today are not designed to provide advanced levels of individual support or real-time knowledge sharing.

"In the not too distant future, you can envision military personnel having a number of sensors on them at any given time – a microphone, a head-mounted camera – and displays like augmented reality (AR) headsets," said Dr. Bruce Draper, a program manager in DARPA's Information Innovation Office (I2O).

"These sensor platforms generate tons of data around what the user is seeing and hearing, while AR headsets provide feedback mechanisms to display and share information or instructions. What we need in the middle is an assistant that can recognize what you are doing as you start a task, has the prerequisite know-how to accomplish that task, can provide step-by-step guidance, and can alert you to any mistakes you're making."

DARPA developed the Perceptually-enabled Task Guidance (PTG) program to explore the development of methods, techniques, and technology for AI assistants capable of helping users perform complex physical tasks.

The goal is to develop virtual "task guidance" assistants that can provide just-in-time visual and audio feedback to help human users expand their skillsets and minimize their errors or mistakes.

To develop these technologies, PTG seeks to exploit recent advances in deep learning for video and speech analysis, automated reasoning for task

and/or plan monitoring, and augmented reality for human-computer interfaces.

“Increasingly we seek to develop technologies that make AI a true, collaborative partner with humans,” said Draper. “Developing virtual assistants that can provide substantial aid to human users as they complete tasks will require advances across a number of machine learning and AI technology focus areas, including knowledge acquisition and reasoning.”

To accomplish its objectives, PTG is divided into two primary research areas.

The first is focused on fundamental research into addressing a set of interconnected problems: knowledge transfer, perceptual grounding, perceptual attention, and user modeling.

The second is focused on integrated demonstrations of those fundamental research outputs on militarily-relevant use case scenarios. Specifically, the program will explore how the task guidance assistants could aid in mechanical repair, battlefield medicine, and/or pilot guidance.

Critical to the program will be the exploration and development of novel approaches to integrated technologies that address four specific technical challenges.

The first is knowledge transfer. Virtual task assistants will need to be able to automatically acquire task knowledge from instructions intended for humans, including checklists, illustrated manuals, and training videos.

The second problem area is perceptual grounding. Assistants need to be able to align their perceptual inputs – including objects, settings, actions, sounds, and words – with the terms the assistant needs to use to describe and model tasks to their human users so that observations can be mapped to its task knowledge. Perceptual attention is the third problem area.

Assistants must be able to pay attention to perceptual inputs that are relevant to current tasks, while ignoring extraneous stimuli. They also need to be able to respond to unexpected, but relevant events that may alter a user’s goals or suggest a new task.

The final problem area is user modeling. PTG assistants must be able to determine how much information to share with a user and when to do so. This requires developing and integrating an epistemic model of what the user knows, a physical model of what the user is doing, and a model of their attentional and emotional states.

Because these four problems are not independent of each other, PTG aims to pursue integrated approaches and solutions that collectively take on all four challenge areas.

The development of AI-enabled agents is not new territory for DARPA. In addition to investing in the advancement of AI technology for more than 50 years, DARPA funded the creation of the technologies that underlie today's virtual assistants, such as Siri.

In the early 2000s, DARPA launched the Personalized Assistant that Learns (PAL) program. Under PAL, researchers created cognitive computing systems to make military decision-making more efficient and more effective at multiple levels of command.

Interested proposers will have an opportunity to learn more about the Perceptually-enabled Task Guidance (PTG) program during a Proposers Day, which will be held on March 18, 2021, from 1:00 PM to 4:45 PM (ET) via Zoom. Advanced registration is required to attend.

To learn more, please visit:
https://beta.sam.gov/opp/cbc9eeedcb39472581bd1d394a97f53d/view?keywords=&sort=-modifiedDate&index=&is_active=true&page=1&organization_id=300000412

The PTG Broad Agency Announcement is forthcoming and will be published on the System for Award Management (SAM) website at https://beta.sam.gov/

Number 10

Advice following Microsoft vulnerabilities exploitation

Urgent updates released for Exchange server vulnerabilities

Microsoft has made public that sophisticated actors have attacked a number of Exchange servers and in response have released multiple security updates for affected servers.

These updates have been released ahead of the monthly update cycle because four of the seven vulnerabilities have been used in limited targeted attacks. The security updates fix the vulnerabilities exploited in the initial attack.

Affected versions

The vulnerabilities affect Microsoft Exchange Server. The versions affected are:

- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019

A defence in depth update for Microsoft Exchange Server 2010 has also been released.

Exchange Online is not affected.

Mitigation

The NCSC recommends following vendor best practice advice in the mitigation of vulnerabilities. In this case, the most important aspect is to install the latest updates immediately.

More information about the security updates can be found on Microsoft's website at:
https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/

msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/

Microsoft Security Response Center

Report an issue

Multiple Security Updates Released for Exchange Server

MSRC / By MSRC Team / March 2, 2021

Today we are releasing several security updates for Microsoft Exchange Server to address vulnerabilities that have been used in limited targeted attacks. Due to the critical nature of these vulnerabilities, we recommend that customers apply the updates to affected systems immediately to protect against these exploits and to prevent future abuse across the ecosystem.

The Microsoft Exchange Server team has published a blog about these updates, which provides a script to obtain an inventory of the patch-level status of Exchange servers on premises. It also assists with some basic questions about installing the security updates.

Further information

Further information, including IOCs and detections, can be found in the Microsoft blogs:

https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks

https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers

Conclusion

The NCSC strongly advises that organisations:

- Read the guidance referenced in this alert
- Install the necessary updates immediately
- Stay informed of any future updates to the guidance from Microsoft (via the links above)

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.

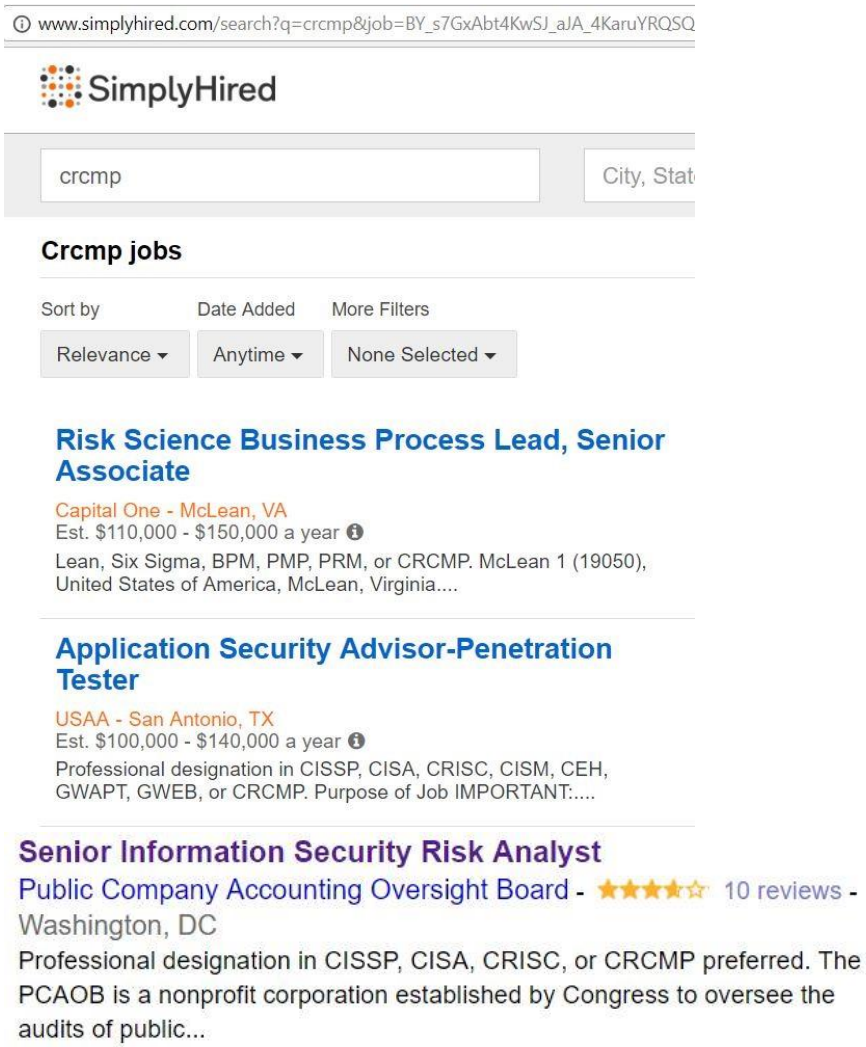
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

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

- 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.