Monday, May 18, 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,

Carl Jung has said that the word happy would lose its meaning if it were not balanced by *sadness*.

According to *Mark Twain,* it is no wonder that *truth* is stranger than fiction. Fiction has to make sense.

Well, it is strange, sad, but also true that Covid-19 is an opportunity.

Regulatory Arbitrage is the practice of taking advantage of a regulatory difference between two or more markets.

Every regulatory difference is an opportunity for regulatory arbitrage. Even the different regulatory approaches for the Covid-19 pandemic can generate alpha, excess return over market performance.

Hedge Funds and financial groups sometimes select the more favourable jurisdictions, playing one government off against another. Some countries understand it. They have a plan, to retain or attract foreign direct investments.

Governments know that hedge fund managers and investment banks like regulator shopping. They try to find the friendliest regime to do business.

Under Basel III, depletion of capital buffers triggers automatic constraints on capital distributions, *although jurisdictions have implemented this in different ways. This is an interesting regulatory difference.*

Recent measures taken by authorities also seek to ensure that *flexibility* in capital requirements and capital conservation go hand in hand. However,

as they are based on *discretionary supervisory actions*, these measures *differ* across a number of dimensions.

According to the Bank for International Settlements (BIS), since the outbreak of the Covid-19 pandemic, authorities worldwide have taken measures to ensure that banks can continue to lend to the real economy.

To that end, they have confirmed that firms should *use capital buffers* to absorb losses, and in addition have granted capital relief in various forms.

Many authorities have restricted distributions of capital, whether through dividends, share buybacks or discretionary bonuses.

The FSI Brief (at number 1 of our list below) describes how regulatory distribution constraints operate under Basel III, and discusses how that standard has been applied in some jurisdictions. Further, it takes stock of recent supervisory actions aimed at capital conservation and discusses *how they differ* across a sample of 14 jurisdictions.

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

Best regards,

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

Number 7 (Page 27)

DARPA Announces Discover DSO Day Webinar

Program managers to discuss areas of interest for potential future scientific and technology research

Number 8 (Page 29)

EIOPA revises its timetable for advice on Solvency II Review until end December 2020

Number 9 (Page 30)

Releasing bank buffers to cushion the crisis - a quantitative assessment

BIS Bulletin No 11, by Ulf Lewrick, Christian Schmieder, Jhuvesh Sobrun and Előd Takáts

Number 10 (Page 32)

FBI El Paso Warns About Scams That Are Targeting the Deceased and Their Grieving Families: Bereavement Scams

Number 1

Banks' dividends in Covid-19 times

Jean-Philippe Svoronos and Rastko Vrbaski

BIS

Highlights

• Regulatory actions in the current circumstances need to focus on preserving banks' lending activity without jeopardising their solvency. This means that flexibility in capital requirements, including through the use of regulatory buffers, and capital conservation should go hand in hand.

• Basel III provides for automatic distribution constraints when capital falls below specific thresholds. In the current context, this may disincentivise firms from following authorities' recommendations to use capital buffers.

• Blanket distribution restrictions imposed through supervisory action may help address these disincentives to the extent that they are not linked to firms' individual capital positions and thus remove any possible stigma effect.

• Most authorities have undertaken initiatives in relation to banks' distribution policies in the Covid19 pandemic environment. However, practices across jurisdictions diverge markedly as regards scope and stringency.

Three different buffers

Basel III provides for three different types of buffer:

(i) a capital conservation buffer (CCoB) that applies to all banks at all times;

(ii) a system-wide countercyclical capital buffer (CCyB) that applies when and to the extent that it is activated by the relevant national authority; and

(iii) a buffer that applies to a bank that is designated as a global or domestic systemically important bank (G-SIB or D-SIB).

All buffers must be met with CET1 that is not already used to meet Pillar 1, Pillar 2 or total loss-absorbing capacity (TLAC) requirements.

The calibration method for these buffers differs, reflecting their different objectives. The CCoB, as a permanently fixed requirement, is set at 2.5% of RWA.

In contrast, the CCyB rate fluctuates. Its level varies between 0% and 2.5% of RWA, depending on how the relevant authority assesses the system-wide risk at any point in time within the credit cycle.

The level of the G-SIB or D-SIB buffer may also vary over time and depends on the systemic importance of the firm within a given financial system.

G-SIBs are identified by the FSB on the basis of a methodology developed by the Basel Committee on Banking Supervision (BCBS) and are allocated to buckets that have increasing requirements for loss absorbency.

These range between 1% and 3.5% of RWA.

D-SIBs are subject to requirements under nationally developed methodologies.

To read more:
https://www.bis.org/fsi/fsibriefs6.pdf

Number 2

High level privacy and security design for NHS COVID-19 Contact Tracing App

Dr Ian Levy, Technical Director, National Cyber Security Centre, UK

National Cyber Security Centre

This document provides a high-level overview of the security and privacy characteristics of the app that is in development by NHSx, the digital innovation unit of the National Health Service, to help manage the COVID-19 crisis in the UK.

This is not a full description of the entire system, the socio-technical design, epidemiological modelling or the plethora of other work being performed outside of this application development. Nor does this document detail the significant, diverse, expert input to the overall system and oversight of its development.

Instead, this technical paper concentrates only on the most important and unique security and privacy characteristics of the putative app and its infrastructure.

We only describe epidemiological and clinical aspects of the system, in order to set context for some technical decisions and trade-offs.

The epidemiological advice and models that the NHS is working from show that self-diagnosis is an important part of managing the spread of the disease, alongside various clinical tests and the wider public health response strategy.

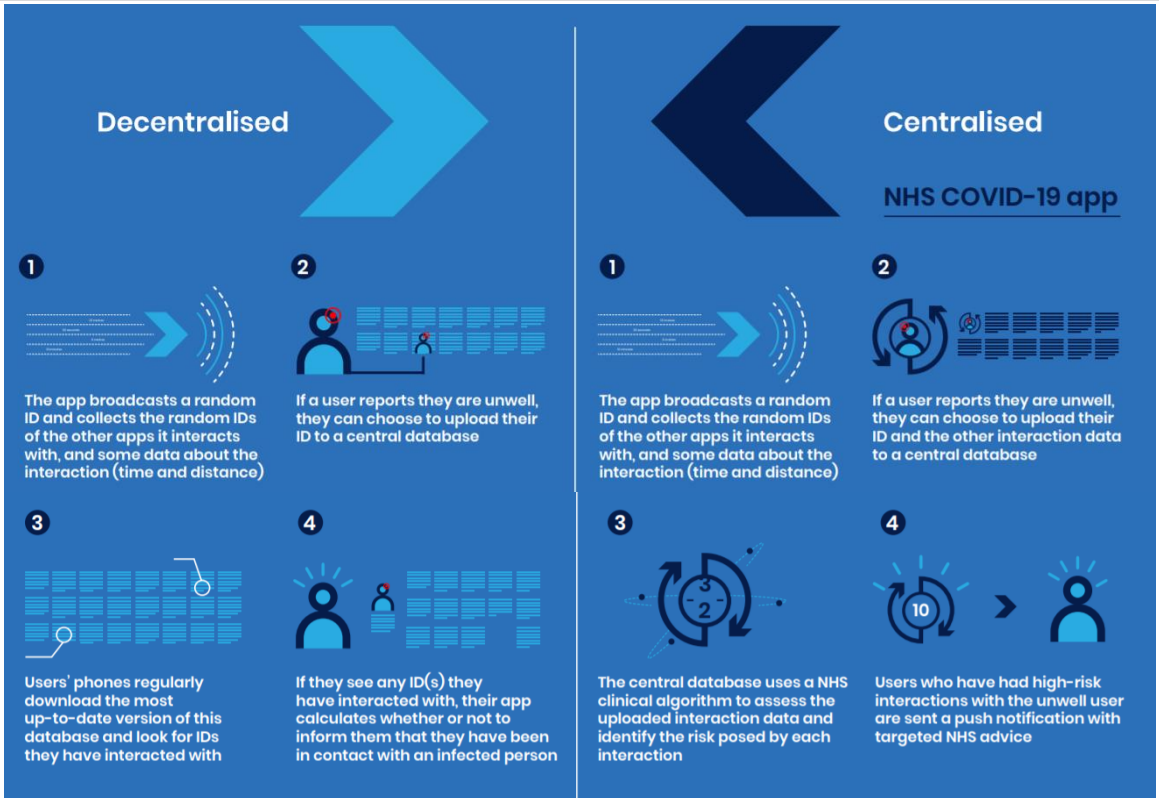
The Oxford group responsible for the model publishes much of its work.

Self-diagnosis can reduce by days, the time it takes a potentially infectious person to isolate.

This is critical to the management of the spread of the disease, under the assumptions in the UK's model.

There are obvious corollaries to a model that includes self-diagnosis. We explore some of those here, with their current mitigations.

Finally, a contact tracing app cannot work in isolation – it must work in concert with, and be a pathway into, the wider public health response. We do not cover that integration here, but it is in place.



Introduction to the NHS COVID-19 app

The NHS COVID-19 app aims to automate key parts of public health contact tracing by offering a proximity cascade system that can help slow transmission of the COVID-19 virus.

This will save lives, reduce pressure on the NHS, help return people to normal life and mitigate damage to the economy.

The app also aims to preserve individual and group privacy, be tolerant to various malicious users and minimise the risks of pseudonymous subgroup reidentification.

Importantly, it is driven by and informs expert epidemiological modelling, which in turn drives public policy.

How the NHSx app works

The user-centric description of the app is: "When I download the app, it keeps an anonymous record of when I've been close to other people (proximity events).
If I self-diagnose in the app, as displaying COVID-19 symptoms, I can choose to provide my personal record of proximity events to an NHSx system.

The NHSx system can then work out who to notify that they have potentially been in contact with COVID-19.

To these people, it can provide the latest advice and, potentially, access to testing.

Analysis of the records of proximity events from people displaying symptoms will allow NHSx to monitor and control the spread of the virus.

To read more:
https://www.ncsc.gov.uk/files/NHS-app-security-paper%20V0.1.pdf

Number 3

Executive Order on Securing the United States Bulk-Power System

whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/

ECONOMY NATIONAL SECURITY BUDGET IMMIGRATION CORONAVIRUS.GOV

EXECUTIVE ORDERS

Executive Order on Securing the United States Bulk-Power System

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 et seq.) (NEA), and section 301 of title 3, United States Code,

I, DONALD J. TRUMP, President of the United States of America, find that foreign adversaries are increasingly creating and exploiting vulnerabilities in the United States bulk-power system, which provides the electricity that supports our national defense, vital emergency services, critical infrastructure, economy, and way of life.

The bulk-power system is a target of those seeking to commit malicious acts against the United States and its people, including malicious cyber activities, because a successful attack on our bulk-power system would present significant risks to our economy, human health and safety, and would render the United States less capable of acting in defense of itself and its allies.

I further find that the unrestricted acquisition or use in the United States of bulk-power system electric equipment designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries augments the ability of foreign adversaries to create and exploit vulnerabilities in bulk-power system electric equipment, with potentially catastrophic effects.

I therefore determine that the unrestricted foreign supply of bulk-power system electric equipment constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States, which has its source in whole or in substantial part outside the United States.

This threat exists both in the case of individual acquisitions and when acquisitions are considered as a class. Although maintaining an open investment climate in bulk-power system electric equipment, and in the United States economy more generally, is important for the overall growth and prosperity of the United States, such openness must be balanced with the need to protect our Nation against a critical national security threat. To address this threat, additional steps are required to protect the security, integrity, and reliability of bulk-power system electric equipment used in the United States. In light of these findings, I hereby declare a national emergency with respect to the threat to the United States bulk-power system.

Accordingly, I hereby order:

Section 1. Prohibitions and Implementation.

(a) The following actions are prohibited: any acquisition, importation, transfer, or installation of any bulk-power system electric equipment (transaction) by any person, or with respect to any property, subject to the jurisdiction of the United States, where the transaction involves any property in which any foreign country or a national thereof has any interest (including through an interest in a contract for the provision of the equipment), where the transaction was initiated after the date of this order, and where the Secretary of Energy (Secretary), in coordination with the Director of the Office of Management and Budget and in consultation with the Secretary of Defense, the Secretary of Homeland Security, the Director of National Intelligence, and, as appropriate, the heads of other executive departments and agencies (agencies), has determined that:

(i) the transaction involves bulk-power system electric equipment designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and

(ii) the transaction:

(A) poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of the bulk-power system in the United States;

(B) poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the economy of the United States; or

(C) otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons.

(b) The Secretary, in consultation with the heads of other agencies as appropriate, may at the Secretary's discretion design or negotiate measures to mitigate concerns identified under section 1(a) of this order. Such measures may serve as a precondition to the approval by the Secretary of a transaction or of a class of transactions that would otherwise be prohibited pursuant to this order.

(c) The prohibitions in subsection (a) of this section apply except to the extent provided by statutes, or in regulations, orders, directives, or licenses that may be issued pursuant to this order, and notwithstanding any contract entered into or any license or permit granted prior to the date of this order.

(d) The Secretary, in consultation with the heads of other agencies as appropriate, may establish and publish criteria for recognizing particular equipment and particular vendors in the bulk-power system electric equipment market as pre-qualified for future transactions; and may apply these criteria to establish and publish a list of pre-qualified equipment and vendors. Nothing in this provision limits the Secretary's authority under this section to prohibit or otherwise regulate any transaction involving pre-qualified equipment or vendors.

Sec. 2. Authorities.

(a) The Secretary is hereby authorized to take such actions, including directing the timing and manner of the cessation of pending and future transactions prohibited pursuant to section 1 of this order, adopting appropriate rules and regulations, and employing all other powers granted to the President by IEEPA as may be necessary to implement this order.

The heads of all agencies, including the Board of Directors of the Tennessee Valley Authority, shall take all appropriate measures within their authority as appropriate and consistent with applicable law, to implement this order.

(b) Rules and regulations issued pursuant to this order may, among other things, determine that particular countries or persons are foreign adversaries exclusively for the purposes of this order; identify persons owned by, controlled by, or subject to the jurisdiction or direction of foreign

adversaries exclusively for the purposes of this order; identify particular equipment or countries with respect to which transactions involving bulk-power system electric equipment warrant particular scrutiny under the provisions of this order; establish procedures to license transactions otherwise prohibited pursuant to this order; and identify a mechanism and relevant factors for the negotiation of agreements to mitigate concerns raised in connection with subsection 1(a) of this order.

Within 150 days of the date of this order, the Secretary, in consultation with the Secretary of Defense, the Secretary of Homeland Security, the Director of National Intelligence, and, as appropriate, the heads of other agencies, shall publish rules or regulations implementing the authorities delegated to the Secretary by this order.

(c) The Secretary may, consistent with applicable law, redelegate any of the authorities conferred on the Secretary pursuant to this section within the Department of Energy.

(d) As soon as practicable, the Secretary, in consultation with the Secretary of Defense, the Secretary of the Interior, the Secretary of Homeland Security, the Director of National Intelligence, the Board of Directors of the Tennessee Valley Authority, and the heads of such other agencies as the Secretary considers appropriate, shall:

(i) identify bulk-power system electric equipment designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary that poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of the bulk-power system in the United States, poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the economy of the United States, or otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons; and

(ii) develop recommendations on ways to identify, isolate, monitor, or replace such items as soon as practicable, taking into consideration overall risk to the bulk-power system.

Sec. 3. Task Force on Federal Energy Infrastructure Procurement Policies Related to National Security.

(a) There is hereby established a Task Force on Federal Energy Infrastructure Procurement Policies Related to National Security (Task Force), which shall work to protect the Nation from national security

threats through the coordination of Federal Government procurement of energy infrastructure and the sharing of risk information and risk management practices to inform such procurement. The Task Force shall be chaired by the Secretary or the Secretary's designee.

(b) In addition to the Chair of the Task Force (Chair), the Task Force membership shall include the following heads of agencies, or their designees:

(i) the Secretary of Defense;
(ii) the Secretary of the Interior;
(iii) the Secretary of Commerce;
(iv) the Secretary of Homeland Security;
(v) the Director of National Intelligence;
(vi) the Director of the Office of Management and Budget; and
(vii) the head of any other agency that the Chair may designate in consultation with the Secretary of Defense and the Secretary of the Interior.

(c) The Task Force shall:

(i) develop a recommended consistent set of energy infrastructure procurement policies and procedures for agencies, to the extent consistent with law, to ensure that national security considerations are fully integrated across the Federal Government, and submit such recommendations to the Federal Acquisition Regulatory Council (FAR Council);

(ii) evaluate the methods and criteria used to incorporate national security considerations into energy security and cybersecurity policymaking;

(iii) consult with the Electricity Subsector Coordinating Council and the Oil and Natural Gas Subsector Coordinating Council in developing the recommendations and evaluation described in subsections (c)(i) through (ii) of this section; and

(iv) conduct any other studies, develop any other recommendations, and submit any such studies and recommendations to the President, as appropriate and as directed by the Secretary.

(d) The Department of Energy shall provide administrative support and funding for the Task Force, to the extent consistent with applicable law.

(e) The Task Force shall meet as required by the Chair and, unless extended by the Chair, shall terminate once it has accomplished the objectives set forth in subsection (c) of this section, as determined by the Chair, and completed the reports described in subsection (f) of this section.

(f) The Task Force shall submit to the President, through the Chair and the Director of the Office of Management and Budget:

(i) a report within 1 year from the date of this order;

(ii) a subsequent report at least once annually thereafter while the Task Force remains in existence; and

(iii) such other reports as appropriate and as directed by the Chair.

(g) In the reports submitted under subsection (f) of this section, the Task Force shall summarize its progress, findings, and recommendations described in subsection (c) of this section.

(h) Because attacks on the bulk-power system can originate through the distribution system, the Task Force shall engage with distribution system industry groups, to the extent consistent with law and national security.

Within 180 days of receiving the recommendations pursuant to subsection (c)(i) of this section, the FAR Council shall consider proposing for notice and public comment an amendment to the applicable provisions in the Federal Acquisition Regulation to implement the recommendations provided pursuant to subsection (c)(i) of this section.

Sec. 4. Definitions.

For purposes of this order, the following definitions shall apply:

(a) The term “bulk-power system” means:

(i) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and

(ii) electric energy from generation facilities needed to maintain transmission reliability. For the purpose of this order, this definition includes transmission lines rated at 69,000 volts (69 kV) or more, but does not include facilities used in the local distribution of electric energy.

(b) The term “bulk-power system electric equipment” means items used in bulk-power system substations, control rooms, or power generating stations, including reactors, capacitors, substation transformers, current coupling capacitors, large generators, backup generators, substation voltage regulators, shunt capacitor equipment, automatic circuit reclosers, instrument transformers, coupling capacity voltage transformers, protective relaying, metering equipment, high voltage circuit breakers,

generation turbines, industrial control systems, distributed control systems, and safety instrumented systems.

Items not included in the preceding list and that have broader application of use beyond the bulk-power system are outside the scope of this order.

(c) The term "entity" means a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization.

(d) The term "foreign adversary" means any foreign government or foreign non-government person engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or its allies or the security and safety of United States persons.

(e) The term "person" means an individual or entity.

(f) The term "procurement" means the acquiring by contract with appropriated funds of supplies or services, including installation services, by and for the use of the Federal Government, through purchase, whether the supplies or services are already in existence or must be created, developed, demonstrated, and evaluated.

(g) The term "United States person" means any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States.

Sec. 5. Recurring and Final Reports to the Congress.

The Secretary is hereby authorized to submit recurring and final reports to the Congress regarding the national emergency declared in this order, consistent with section 401(c) of the NEA (50 U.S.C. 1641(c)) and section 204(c) of IEEPA (50 U.S.C. 1703(c)).

Sec. 6. General Provisions.

(a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

DONALD J. TRUMP,
THE WHITE HOUSE,

Number 4

G20 TechSprint

TechSprint is a joint initiative of the BIS Innovation Hub (BISIH) and the Saudi G20 Presidency designed to showcase the potential for new innovative technologies to resolve operational problems in the areas of regulatory compliance (RegTech) and supervision (SupTech).

It is being implemented with the support of the Monetary Authority of Singapore (MAS), the Saudi Arabian Monetary Authority (SAMA), the Financial Stability Board (FSB), API Exchange (APIX), and Regtech for Regulators Accelerator (R2A).

Its purpose is to showcase the potential for new innovative technologies to resolve operational problems in the areas of regulatory compliance (RegTech) and supervision (SupTech).

In TechSprint, the BISIH has published selected problem statements and invites private firms to develop technological solutions to these problems.

Regulatory reporting

Regulatory reporting and ensuring compliance: With increasing digitalisation, are there upstream solutions and tools that would enable regulators to easily prepare and transmit machine-readable and machine-executable regulations to their regulated entities (i.e. codified regulations that are sent to regulated entities that would allow for regulatory data to be easily and autonomously mined and reported).

This should result in greater regulatory compliance, lower regulatory burden and cost, improve data quality and consistency in regulatory reporting, as well as engender more timely surveillance by the regulatory authorities.

Solutions should be deployable at least within a jurisdiction (with teams responsible for demonstrating this ability), and configurable for deployment across multiple jurisdictions, especially in areas of regulation where there are internationally accepted and harmonised data requirements (e.g. established data identifiers such as the Legal Entity Identifier Regulatory Oversight Committee (LEI ROC), the Unique Transaction (UTI) and the Unique Product Identifier (UPI)).

Solutions could also include the development of a common code repository shared between the regulators and regulated entities to push and pull required regulatory reports/data via authorised APIs.

Monitoring and Surveillance

Monitoring AML/CFT Risks: Crypto assets have garnered significant interest from the financial industry. However, AML/CFT risk in the crypto asset space has been a constant concern for regulators.

How can AI (artificial intelligence), ML (machine-learning), data visualisation tools and other technologies help financial institutions conduct better monitoring and report suspicious activities in more timely and accurate manner for AML/CFT purposes, as well as help crypto assets service providers comply with AML/CFT regulations?

A particular area of interest would be tools to monitor against AML/CFT risks at the main fiat-to-crypto conversion gateways (i.e. help gatekeepers identify suspicious users/transactions in a timely and accurate manner).

Dynamic Information sharing

Utilizing Innovation to support the efforts in response to Covid-19

On March 6, 2020 G20 Finance Ministers and Central Bank Governors issued a statement on COVID-19 stating that they will work closely with the relevant international organizations with a view to sharing information, among other key areas of collaboration.

The G20 TechSprint aspires to contribute to the information sharing element, with the view to supporting effective collaboration amongst financial supervisors and regulators across borders given the global reach of the pandemic.

The COVID-19 pandemic is unprecedented and has called for extraordinary measures by all stakeholders to mitigate further risks by supporting households and businesses.

The effectiveness of these measures calls for strong and frequent coordination and cooperation amongst financial regulators and supervisors.

To that end, the G20 TechSprint puts forward the following problem statement.

Dynamic Information Sharing for Supervisors and Regulators in Response to Crises (both natural or man-made) that Impact Global Financial Stability:

Since the onset of the Covid-19 global pandemic, supervisors and regulators have been coordinating on a frequent basis with the aim of supporting the global economy by ensuring the continued functioning of our global financial system.

The pandemic has called for a dynamic response, where regulatory and supervisory measures are implemented on an almost daily basis.

Can a technological solution be developed to facilitate the sharing of critical information among regulators and supervisors?

Through the use of an application that sources both structured data (e.g. financial regulatory reports) and publicly available information that may be unstructured (e.g. releases on national authorities' websites on regulatory and supervisory measures in response to the crisis, market feeds on developing events and social media sources, etc) on a near real-time basis.

The solution should offer a comprehensive overview of the measures undertaken within and across jurisdictions in terms of the regulatory and supervisory responses, categorized across the different components of the financial system.

This solution should be applicable and deployable in response to a crisis that could have an impact on global financial stability.

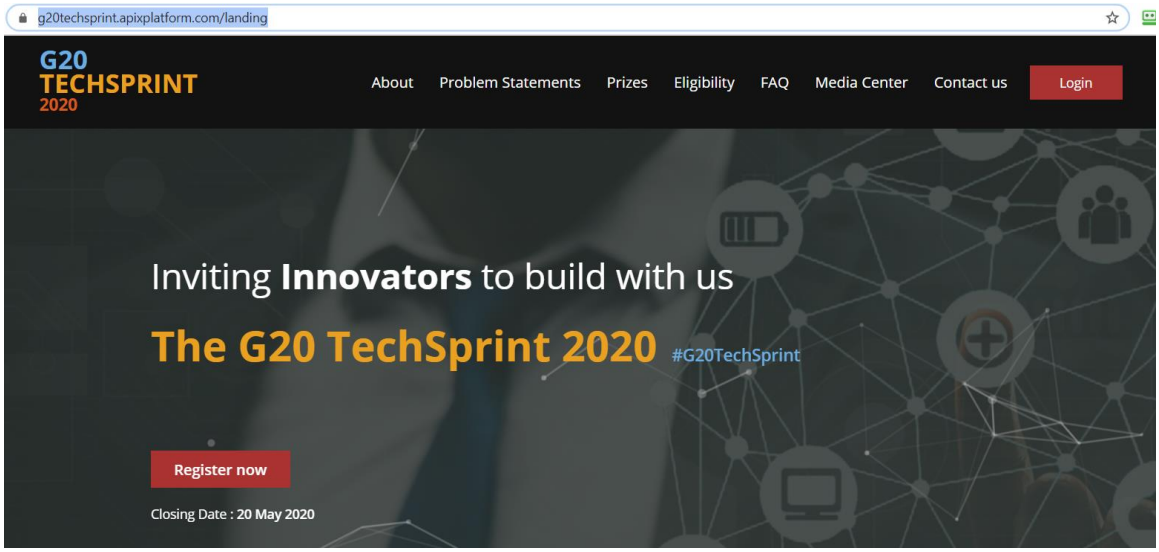
An ideal solution would incorporate user-friendly interface, with a searchable database on supervisory and regulatory measures currently in place, and dashboarding tools that would allow for context and customisations based on differing user requirements (e.g. focus by regions and/or on different focal parameters such as capital and liquidity risk).

Solutions that take advantage of machine learning to increase the speed of accurately filtering between noise and signals would aid effective monitoring of market developments, especially in these critical moments.

A bonus outcome of the solution is if it could also be easily deployed for regulatory oversight at the level of individual firms, such as in aiding supervisors to quickly assess and diagnose the level of risk to specific financial institutions.

Interested private firms can compete and develop innovative solutions to these problems using the cloud-based APIX platform that facilitates registration, prototype building and online judging of submissions.

An independent international expert panel will choose the winning solutions, which will then be showcased at fintech festivals.



You may visit:
https://www.g20techsprint.apixplatform.com/landing

Number 5

FSB consults on guidance on assessing the adequacy of financial resources for CCP resolution

The Financial Stability Board (FSB) has published a public consultation report on Guidance on financial resources to support CCP resolution and on the treatment of CCP equity in resolution.

The guidance will assist central counterparty (CCP) resolution authorities.

Central clearing of standardised over-the-counter (OTC) derivatives is a key pillar of the G20 Leaders' commitment to reform OTC derivatives markets in response to the 2008 financial crisis.

Increased central clearing has simplified the previously complex and opaque web of derivatives exposures.

In addition, more collateral is in place to reduce counterparty credit risks.

At the same time, CCPs' criticality to the overall safety and soundness of the financial system means that authorities must take steps to ensure that CCPs do not themselves become a source of systemic risk and that they can be successfully resolved without exposing taxpayers to loss.

The draft guidance is based on the concepts included in a discussion paper the FSB published in 2018. It takes into account the comments received in that earlier public consultation and feedback from the resolution authorities of CCPs.

Part I of the guidance proposes five steps to guide the authorities in assessing the adequacy of a CCP's financial resources and the potential financial stability implications of their use.

The authorities should:

Step 1: identify hypothetical default and non-default loss scenarios (and a combination of them) that may lead to a resolution of a CCP;

Step 2: conduct a qualitative and quantitative evaluation of existing resources and tools available in the resolution of the CCP;

Step 3: assess potential resolution costs;

Step 4: compare existing resources and tools to resolution costs and identify any gaps; and

Step 5: evaluate the availability, costs and benefits of potential means of addressing any identified gaps.

Part II of the guidance addresses the treatment of CCP equity in resolution. It provides a framework for resolution authorities to evaluate the exposure of CCP equity to losses in recovery, liquidation and resolution and how (where it is possible) the treatment of CCP equity in resolution could be adjusted.

The FSB welcomes responses to the questions set out in the public consultation report by 31 July 2020.

To learn more:
https://www.fsb.org/wp-content/uploads/P020520.pdf

Number 6

Understanding and dealing with phishing during the covid-19 pandemic

Many organisations and companies experience changes in their working conditions lately due to the COVID-19 pandemic. This shift has increased remote activities, such as teleworking. Teleworking furthers the reliance on email for communication, thus creating perfect conditions for email fraud schemes.

Cyber criminals are taking advantage of the pandemic by using widespread awareness of the subject to trick users into revealing their personal information or clicking on malicious links or attachments, unwittingly downloading malware to their computers. They may even impersonate government organisations, ministries of health, centres for public health or important figures in a relevant country in order to disguise themselves as reliable sources.

The emails look authentic and may include logos or branding of the specific organisations.

How scammers operate

Malicious email messages that might ask you to open an attachment supposedly containing pertinent information regarding the Coronavirus are likely to download malicious software onto your device as soon as you click on the attachment or embedded link.

This software could allow cybercriminals to take control of your computer, log your keystrokes or access your personal information and financial data, which could lead to identity theft.

How to recognize phishing

The emails sent usually:

- look identical to messages from a reputable organisation (such as a medical or governmental institution),

- sound urgent or try to spread fear,

- claim to enclose important information or breaking news,

- ask you to download and/or click on attachments and links.

How to Protect against Phishing Attacks

There are simple steps you can take to avoid the bait:

1) Take time to reflect on a request for your personal information and whether the request is appropriate. Do not open unsolicited email from people unfamiliar to you or click on suspicious attachments, which you did not expect.

2) Never supply any personal or financial information and passwords to anyone via email.

3) Avoid emails that insist you act now. Phishing emails often try to create a sense of urgency or demand immediate action.

4) Look for wording and terminology. Apart from phishing, cyber criminals could also trap a specific person via spear phishing using the receiver's full name. Check for terms and language that is normally expected in the type of email you receive.

5) Check the email address. Check the sender's name, email address and whether the email domain matches the organisation that the sender claims to be from. If not, it is probably a phishing attempt.

6) Check the link before you click. See your emails in plain text to check for the hyperlinked address to see the real hyperlink. If it is not the same as what appears in the email, it is probably a phishing attempt.

7) Keep an eye out for spelling and grammatical mistakes. If an email includes spelling, punctuation and/or grammar errors, it could be a phishing email.

8) Be wary of third-party sources spreading information about COVID-19. Refer to the official websites for updates on COVID-19. Fraudulent e-mails can look like they come from a real organisation but legitimate government agencies will never call you or email you directly for this information.

9) Protect your devices. Install anti-spam, anti-spyware and anti-virus software and make sure they are always up to date.

10) Visit websites by typing the domain name yourself. Most businesses use encryption and Secure Socket Layer (SSL) / Transport Layer Security (TLS). If you receive a certificate error while browsing, consider it as a warning sign that something is not right with the website.

What happens if I became a victim of phishing?

- If you have clicked on a link or opened an attachment that downloaded harmful software, update your computer's security software and run a scan.

- If you entered login credentials to access information, change them immediately.

- If you have provided your bank details, contact your bank or credit card company.

Take actions

COVID-19 has affected millions of people around the world, while its long-term impact remains to be seen. However, protecting ourselves against coronavirus-related scams is both a feasible and essential step. If you receive a phishing email, you should:

1. Report it to your IT department by forwarding it as an attachment.
2. Delete it.
3. Notify the organization being spoofed in order to prevent other people from being victimized.

Number 7

DARPA Announces Discover DSO Day Webinar

Program managers to discuss areas of interest for potential future scientific and technology research

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

The Defense Sciences Office (DSO) – one of six technical offices at DARPA – is sponsoring Discover DSO Day (D3) via webinar June 24-25, 2020, to inform potential proposers about the scientific and technical research areas of interest to DSO.

Defense Sciences Office (DSO)

"The goal of D3 is to familiarize attendees with DSO's mission, provide an overview of the latest office-wide Broad Agency Announcement (BAA) solicitation scheduled for release in June, and facilitate dialogue between our program managers and participants," said DSO Director Valerie Browning. "While we aren't able to host the event in person due to the COVID-19 pandemic, we're looking forward to an informative and interactive on-line event."

DSO identifies and pursues high-risk, high-payoff research initiatives across a broad spectrum of science and engineering disciplines and transforms them into important, new game-changing technologies for U.S. national security.

Current DSO themes, which will be discussed at D3, include frontiers in math, computation, and design; limits of sensing and sensors; complex social systems; and anticipating surprise. DSO relies on the greater scientific research community to help identify and explore ideas that could potentially revolutionize the state of the art.

On day one of the event, DSO program managers will give presentations outlining their research interests followed by an audience question and answer session.

Additional presentations will cover how to do business with DARPA, Contracting 101, and DSO's Disruptioneering opportunities. An interactive session with the DSO director will conclude the first day.

Day two is designated for prescheduled individual sidebar video meetings with DSO program managers. A separate, earlier Special Notice announced opportunities for attendees to potentially have sidebar meetings with DSO program managers. This Special Notice has closed, and recipients of sidebar meetings have been notified; no additional sidebars will be scheduled during the D3 event.

The full agenda and registration details for the event are available here: https://go.usa.gov/xvdv8

Number 8

EIOPA revises its timetable for advice on Solvency II Review until end December 2020

EIOPA, in close coordination with the European Commission, has decided to deliver its advice to the European Commission at end December 2020, to take into account the importance of assessing the impact of the current Covid-19 situation on the Solvency II Review.

EIOPA earlier announced on 17 March 2020 that, in order to offer operational relief in reaction to the Covid-19 pandemic, the deadline of the information request for the holistic impact assessment of the 2020 Solvency II Review would be extended by two months, to 1 June 2020. You may visit:
https://www.eiopa.europa.eu/content/eiopa-statement-actions-mitigate-impact-coronaviruscovid-19-eu-insurance-sector

The new timing will allow an update of the holistic impact assessment in view of the impact of the pandemic on the financial markets and insurance business and to take that impact into account in EIOPA's advice.

The new timing strikes a balance between the need to use the opportunity of reviewing the Solvency II directive and the need for the advice to reflect recent developments.

In order to update the holistic impact assessment EIOPA will complement the ongoing information request with a collection of data with a reference date of 30 June 2020.

That information request will be carried out from July to mid-September 2020. It will be addressed to a sub-sample of those subject to the ongoing information request and will be more focussed than that request.

EIOPA will continue to monitor the crisis and its impacts and will engage with all stakeholders in order to ensure a transparent process.

Number 9

Releasing bank buffers to cushion the crisis - a quantitative assessment

BIS Bulletin No 11, by Ulf Lewrick, Christian Schmieder, Jhuvesh Sobrun and Előd Takáts

BIS

- Banks globally entered the Covid-19 crisis with roughly US$ 5 trillion of capital above their Pillar 1 regulatory requirements.

- The amount of additional lending will depend on how hard banks' capital is hit by the crisis, on their willingness to use the buffers and on other policy support.

- In an adverse stress scenario such as the savings and loan crisis, banks' usable buffers would decline to US$ 800 billion, which could support US$ 5 trillion of additional loans (6% of total loans outstanding). Yet in a severely adverse scenario, similar to the Great Financial Crisis, the corresponding figures would be only US$ 270 billion and US$ 1 trillion (1.3% of total loans).

Composition of CET1 capital requirements and release potential[1] Table 1

Component	**Level** (CET1/RWA)	**Release potential** (US$ trillions)
Minimum Basel III requirement	4.5%	n/a
Capital conservation buffer (CCoB)	2.5%	Used only temporarily to cope with stress
G-SIB and D-SIB buffer (SIB buffer)	0.6%	Used only temporarily to cope with stress (G-SIB); design-dependent (D-SIB)
Countercyclical capital buffer (CCyB)	0.2%	0.1
Supervisory and management buffers[2]	6.2%	5.0
CET1 capital ratio (end-2019)	14.0%	5.1

[1] Based on 5,598 banks with total assets of US$ 165 trillion at end-2019; averages are weighted by total assets. [2] Comprise (undisclosed) Pillar 2 buffers and capital in excess of supervisory requirements ("management buffer").

Sources: FitchConnect; authors' calculations.

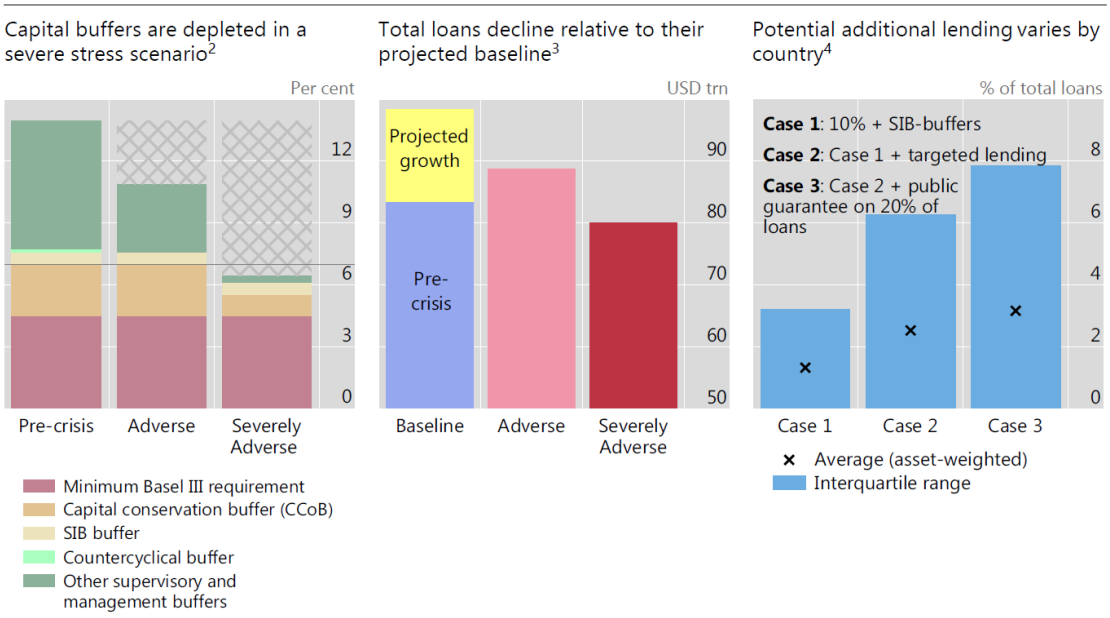
History does not repeat itself, but it often does rhyme – as Mark Twain reminisced. Even though the Covid19 crisis is exceptional in many ways, the GFC and other banking crises since the 1990s provide some guidance on the capital depletion that banks could suffer over the coming years as the crisis unfolds.

We consider two stress scenarios. The approach builds on Hardy and Schmieder (2013), who propose "rules of thumb" for robust bank stress tests based on banking crises since the 1990s.

The first scenario, referred to as the adverse scenario, assumes losses on existing loans comparable to those resulting from the savings and loan crisis in the United States. The second one, the severely adverse scenario, considers losses roughly equivalent to those observed for the GFC.

Capital ratios are projected to fall substantially in both scenarios (Graph 2, left-hand panel). Specifically, the average capital ratio would fall from the current 14% CET1/RWA to 10.9% and 6.5% in the adverse and severely adverse scenario, respectively.

Macroeconomic scenarios and additional lending supported by usable buffers[1] Graph 2



[1] Based on a sample of 5,598 banks at end-2019. [2] The horizontal line represents a CET1 capital ratio of 7% (Basel III minimum requirement and CCoB). [3] The panel depicts the amount of total loans for three scenarios: the baseline (first bar) is equal to the pre-crisis level of loans (ie at end-2019) to which we add the projected increase in loans over three years (the stress horizon) using the pre-crisis trend growth. The second and third bars present the level of total loans under adverse and severely adverse stress. Credit grows more slowly than in the baseline scenario and banks write off loans based on the trajectories in Hardy and Schmieder (2013). The additional loans that banks could extend based on their usable buffers are considered separately (Table 2; and Graph 2, right-hand panel). [4] The graph shows the amount of additional loans in the severely adverse scenario (centre panel) that banks could issue as a percentage of total loans at the country level. The graph compares three cases: banks running down their CET1 ratios to 10% + SIB buffers (Case 1); banks using all the capital released under Case 1 for lending (Case 2); and banks, on top of that, receiving a public guarantee on 20% of all additional loans (Case 3).

Sources: FitchConnect; authors' calculations.

To read more:
https://www.bis.org/publ/bisbull11.pdf

Number 10

FBI El Paso Warns About Scams That Are Targeting the Deceased and Their Grieving Families: Bereavement Scams

Losing a loved one can take an enormous toll—physically, emotionally, and even financially. It is hard enough on its own without also having to worry about fraud on top of it. Scammers will try to cash in on your already-difficult situation.

The fraudster could try to open new credit cards in the deceased person's name or use a phishing scheme to pressure a grieving spouse into paying for a bogus benefit.

Perhaps he says that he is calling from an insurance company and is able to re-instate an expired life insurance policy if she just makes a payment to cover the last few years of unpaid fees. ID thieves may even try to use the deceased person's Social Security number to create a new identity.

There are many versions of these types of scams to include: outstanding debt, funeral scams, Medicare scams, tax fraud, romance/compassion scams, delinquent Life Insurance ploys, credit card scams, and possibly specially engraved trinkets.

So how do you protect your family after the loved one has passed?

We all want to acknowledge a loved one's life completed. But be aware of how many personal facts you provide in an obituary, post online, including social media, the greater the risk of scams—for the departed and survivors alike.

When it's time to write your loved one's obituary, give the deceased's age, but leave out the birthdate, middle name, home address, birthplace, and mother's maiden name. This part will be hard to follow, don't include the names of family survivors. This may open them up to these scams.

Each day, thousands of deceased family members fall victim to identity theft— costing their survivors pain and financial loss.

Alert the major credit reporting agencies as soon as you can as to the passing of your loved one.

They will want copies of the death certificate as well as specific details about your relative, including date of birth, Social Security Number, full legal name, and recent addresses.

The agencies will flag the person's credit file and put a freeze on it to prevent others from opening new unauthorized lines of credit.

Obtain a credit report for the deceased person right after death and a few months afterwards. This will help you to identify any otherwise unknown accounts and to watch out for any attempted fraudulent activity after death.

Make sure to also notify any current banks, credit unions, or financial institutions that the deceased person used so that all checking, savings, investment, or credit card accounts can be flagged appropriately.

The same thing for insurance companies holding auto, home, or life insurance policies. Check with the financial institution to see what access survivors' are entitled to and what protections will be put in place to keep scammers out.

Send a copy of the death certificate to the IRS so that the person's tax account can be flagged as well. Send the death certificate to the mailing address that the deceased individual would normally use to submit tax returns. You may also submit a copy of the death certificate when you file the person's final tax return.

Sometimes your funeral home will notify the Social Security Administration — but if not, you should do so right away.

In a time that should be dedicated to healing, many families are instead sorting through confusing, and often convincing, forms of deceit. Still, if you know what to look for, you can avoid being swindled and focus on finding grief support.

As always, if you have been victimized by a cyber fraud, you can report it to the FBI's Internet Crime Complaint Center at www.IC3.gov

Disclaimer

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

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

This information:

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

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

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

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

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

- is in no way constitutive of an interpretative document;

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

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

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

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

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

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

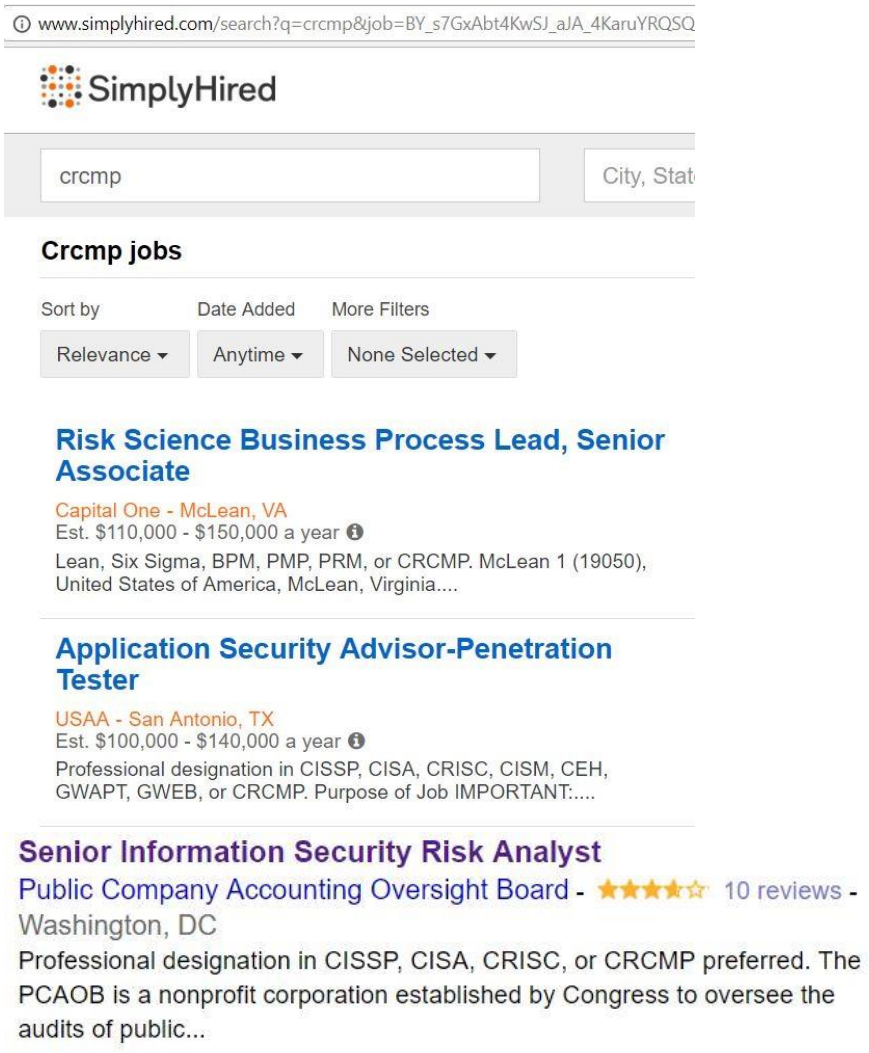
International Association of Risk and Compliance Professionals

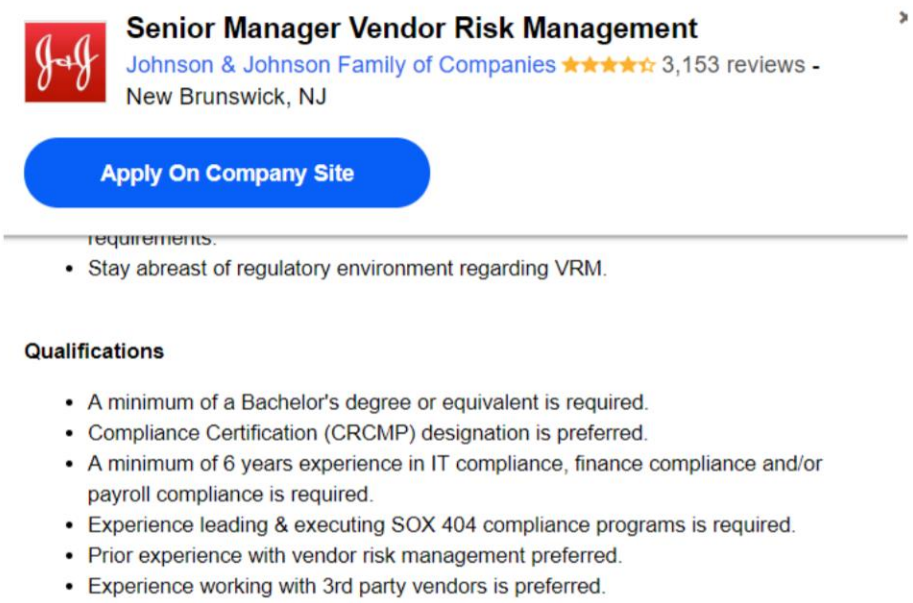
You can explore what we offer to our members:

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

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

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





Senior Manager Vendor Risk Management

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

Apply On Company Site

requirements.

- Stay abreast of regulatory environment regarding VRM.

Qualifications

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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