Monday, December 14, 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,

We have some interesting observations in the new paper with title: *"Staff Observations and Reminders during the COVID-19 Pandemic",* from the Public Company Accounting Oversight Board (PCAOB).

As we know, a review of interim financial information consists principally of the auditor performing analytical procedures and making inquiries.

If the auditor becomes aware of information that leads him or her to believe that the interim financial information may not be in conformity with Generally Accepted Accounting Principles in all material respects, the auditor should make additional inquiries or perform other procedures that he or she considers appropriate to provide a basis for communicating whether he or she is aware of any material modifications that should be made to the interim financial information.

According to the paper, the PCAOB observations include:

1. In addition to formally consulting in accordance with firm policies and procedures, many engagement teams increased their interactions with firm industry leaders, national office personnel, or other engagement teams regarding COVID-19 related accounting and auditing issues.

2. Engagement teams' interactions with audit committees have increased in frequency during the reviews of interim financial information.

Many of these communications with audit committees relate to the effects of the pandemic on the public company's interim financial statements,

including accounting policies and practices and its internal control over financial reporting.

3. Engagement teams considered various methodologies to establish materiality in response to changes in key metrics for both their interim financial information reviews, and to plan the nature, timing, and extent of audit procedures.

In addition, engagement teams consulted when quantitative and qualitative factors previously used to determine materiality changed significantly.

4. Certain engagement teams expanded their use of fraud and forensic specialists during fraud brainstorming sessions and planning.

5. As engagement teams performed reviews of interim financial information, they have, in many instances, focused their analytical procedures, inquiries, and other procedures on the public company's ability to continue as a going concern and the potential for impairment of goodwill and other long-lived assets.

Engagement teams often involved auditor specialists, including forensic specialists, to assist in reviewing certain higher risk areas, including significant assumptions in accounting estimates such as those related to projected financial information.

Some engagement teams also engaged in discussions with the company's specialists regarding valuations performed.

6. Many engagement teams began planning for inventory observations early in the audit process, including by consulting with national office resources on an appropriate audit strategy and engaging with the public company's management.

In one instance, an engagement team performed a real-time virtual inventory observation, using known landmarks to verify the location.

In another instance, an engagement team conducted a "dry run" virtual inventory observation with the public company's management in advance of the year-end physical inventory observation to test the technology they intended to use.

7. Engagement teams used virtual meetings, screen-sharing tools, instant messaging, and related technologies to communicate with one another.

In some cases, team members were connected through an all-day virtual meeting to simulate a "work room" environment that enabled ad hoc communication and facilitated supervision of the work of engagement team members.

This is an interesting approach. Stephen Hawking has said that intelligence is the ability to adapt to change.

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

Best regards,

George Lekatis

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

Number 1 (Page 6)

PCAOB Issues COVID-19 Spotlight, Provides Insights and Reminders for Auditors

Number 2 (Page 8)

Telecom Security During a Pandemic

Telecom security good practices and lessons learned from the COVID-19 outbreak

Number 3 (Page 11)

Preparation for permanent cessation of LIBOR

Japanese FSA

Number 4 (Page 13)

Federal Reserve Board welcomes and supports release of proposal and supervisory statements that would enable clear end date for U.S. Dollar (USD) LIBOR and would promote the safety and soundness of the financial system

Number 5 (Page 15)

EIOPA launches discussion paper on a methodology for integrating climate change in the standard formula

Number 6 (Page 17)

Why Islamic finance has an important role to play in supporting the recovery from Covid – and how the Bank of England's new Alternative Liquidity Facility can help

Andrew Hauser, Executive Director for Markets of the Bank of England, at the Markets UK Islamic Finance Week 2020, London.

Number 7 (Page 20)

Advanced Persistent Threat Actors Targeting U.S. Think Tanks

Number 8 (Page 25)

Face Recognition Software Shows Improvement in Recognizing Masked Faces

Latest NIST test is the first to measure performance of software submitted after pandemic's arrival.

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

Number 9 (Page 28)

K9 Chemistry: A Safer Way to Train Detection Dogs

Canine trainers may no longer need to handle or expose dogs to real explosives and narcotics.

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

Number 10 (Page 31)

DARPA Looks to Light up Integrated Photonics with Chip-Scale Laser Development

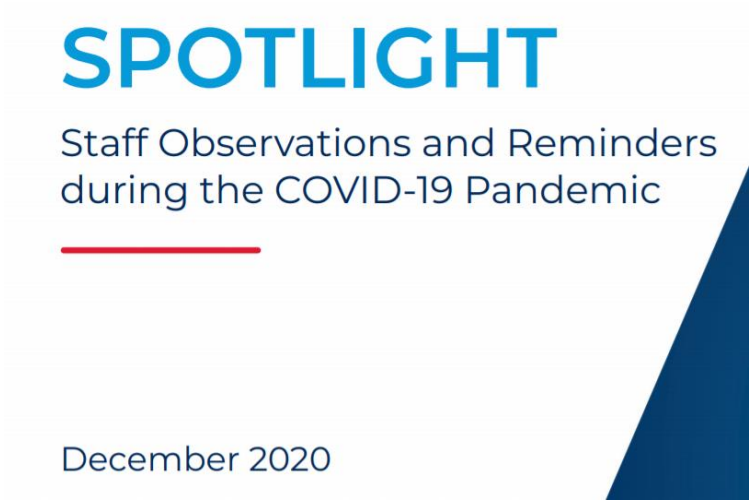
DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 1

PCAOB Issues COVID-19 Spotlight, Provides Insights and Reminders for Auditors

The Public Company Accounting Oversight Board (PCAOB) released a new Spotlight publication, Staff Observations and Reminders during the COVID-19 Pandemic(PDF), to provide insights from recent PCAOB inspections of reviews of interim financial information and audits.

You may visit:
https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/documents/staff-observations-reminders-covid-19-spotlight.pdf?sfvrsn=b14c0d8_6



"Consistent with our strategic objective to conduct inspection activities that facilitate more timely and relevant feedback to our stakeholders, we adjusted our 2020 inspections approach to learn how the COVID-19 crisis is impacting audits," said PCAOB Chairman William D. Duhnke III.

"We encourage auditors to review this Spotlight, which discusses the lessons we learned, as they plan and conduct audits and reviews of interim financial information in the current environment."

This new publication builds on information provided in the PCAOB's April 2020 Spotlight, COVID-19: Reminders for Audits Nearing Completion at https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/documents/covid-19-spotlight.pdf?sfvrsn=24e6b033_0).

Despite the ongoing challenges created by the pandemic, auditors remain responsible for conducting audits in accordance with PCAOB standards and

rules, as well as other regulatory and professional standards. Although the staff observations in this publication relate to audits of public companies, many of the reminders, even where the term "public company" is used, may also be applicable to audits of broker-dealers.

For more COVID-19 related updates and information, visit the PCAOB's resource page at: https://pcaobus.org/about/response-to-covid-19

Number 2

Telecom Security During a Pandemic

Telecom security good practices and lessons learned from the COVID-19 outbreak

The COVID-19 pandemic triggered major changes in the use of electronic communication networks and services in the EU: employees working from home instead of in the office, children receiving home-schooling, citizens using streaming services for entertainment instead of going out, people meeting up over a video link instead of in person, etc.

The security and resilience of electronic communication networks and services became even more important for the EU's society and economy.

In this paper, we look at the role telecom providers played in ensuring the security and resilience of the services and networks during the pandemic.

This paper focuses on the telecom networks and services themselves, not the endpoints. So COVID-related cyberattacks like COVID phishing emails and scam domain names are out of scope here.

Also we don't discuss the arson attacks on base stations inspired by the conspiracy theories about the pandemic.

Throughout this paper we give examples of good practices and we conclude with lessons learned. We look at the following three aspects.

- *Early response phase:* in this phase, providers activated their business continuity plans and supported emergency communications and public warnings. We give examples of such activities in the EU and across the globe.

- *From initial strain to the new normal:* providers had to deal with major surges and shifts in usage and traffic patterns from the start of the pandemic. This gradually stabilised to what is now considered the new normal. We look in detail at the changes in usage and traffic patterns and the network performance monitoring during the pandemic, and examine how providers managed the increased network loads.

- *Response by the national authorities and collaboration with the sector:* we give a brief country-by-country summary of the pandemic

response by the national telecom security authorities in the EU and we give examples of collaboration initiatives and information sharing between providers and authorities as well as in the private sector.

The general take away from the pandemic so far is that the services and the networks have been resilient during the crisis, despite major changes in usage and traffic.

The pandemic also had a lasting effect on the perception of consumers about telecoms: Electronic communication networks are now considered as a lifeline for citizens and they are crucial to keep the economy and society going.

INITIAL CHANGES IN USAGE AND TRAFFIC PATTERNS

- An initial spike in traffic volumes as users attempted to be informed and connected with family and friends.
- Increased consumption of voice services along with a significant drop in the volume of mobile handoffs.
- Increased and persistent upstream traffic volumes as a result of increased use of online collaboration tools for remote work and schooling.
- Usage hotspots in business and commute areas relocated to residential and rural areas.
- A persistent and long-lasting burden on the network, measured in weeks and months.

Figure 1: A schema of the volume of traffic on the telecommunications networks as the pandemic evolved (*Source*: Fastly)

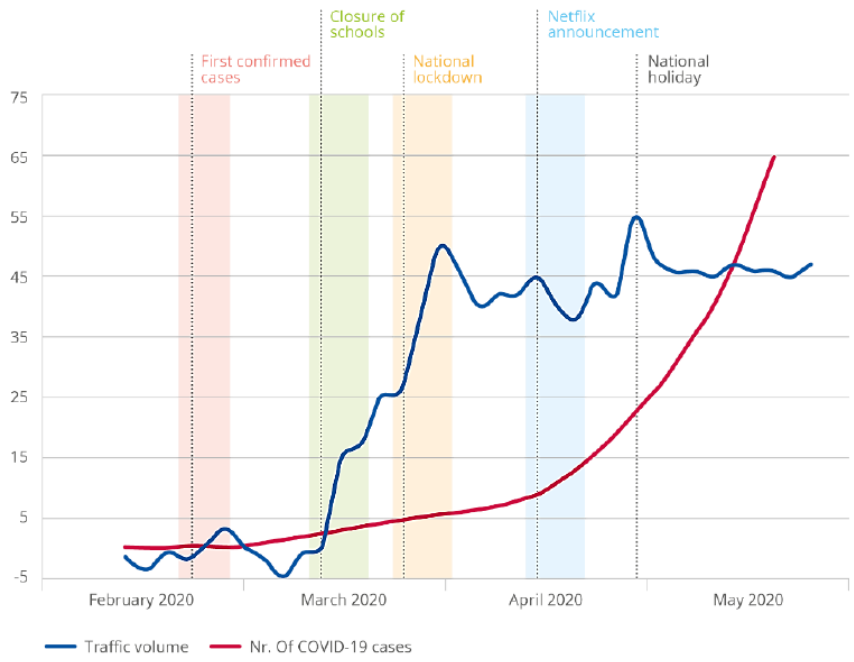
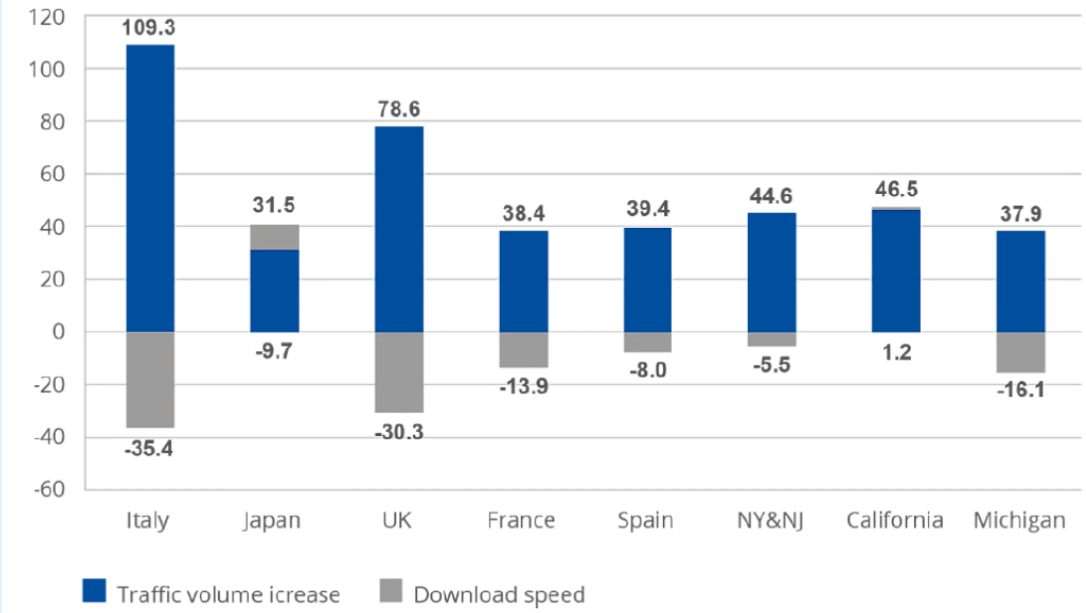


Figure 5: Increased internet traffic volumes in selected European countries and US states that were significantly hit by the pandemic, and the corresponding download speed deteriorations (Source: Fastly)



The paper:
https://www.enisa.europa.eu/publications/telecom-security-during-a-pandemic

Number 3

Preparation for permanent cessation of LIBOR

Japanese FSA

Financial Services Agency

Whereas reforming interest rate benchmarks have been developed in Japan and abroad, the possibility that the London Interbank Offered Rate (LIBOR) will be permanently discontinued after the end of 2021 has been increasing.

While LIBOR is mainly referenced in derivative contracts such as interest rate swaps, it is also quoted in a significant number of cash products including corporate loans and bonds.

Additionally, it is used in wide range of users, including not only financial institutions but also non-financial corporate and institutional investors. In this regard, there is the possibility of disruption to users if LIBOR were ceased without sufficient preparation.

Through close cooperation with the Bank of Japan and other relevant institutions, the Financial Services Agency of Japan (JFSA) will publish or provide links to related materials to help market participants, including financial institutions and non-financial corporate and institutional investors better understand the necessity of taking actions in preparation for the cessation of LIBOR, and also support market-led initiatives for a smooth transition away from LIBOR.

What happened before - Letters to the CEOs of Major Financial Institutions regarding LIBOR Transition

Financial Services Agency of Japan, together with the Bank of Japan, has written to the CEOs of major financial institutions regarding LIBOR transition.

The purpose of sending the letters is to urge financial institutions to take actions for permanent cessation of LIBOR and to request submission of relevant materials to review the progress of preparedness in individual firms.

As mentioned above, the letters have been sent to some financial institutions. However, we will monitor preparedness of other financial institutions based on the contents of the letters.

Any financial institutions using LIBOR are expected to accelerate their actions by responsible and active involvement of management officials with due consideration for description of the letters.

The letter:
https://www.fsa.go.jp/en/policy/libor/dearceoletter20200601_en.pdf

Dear CEO of the Financial Institution

MORITA Tokio, Director-General,
Strategy Development and Management Bureau, Financial Services Agency

KURITA Teruhisa, Director-General,
Supervision Bureau, Financial Services Agency

KOGUCHI Hirohide, Director-General,
Financial System and Bank Examination Department, Bank of Japan

Taking Actions for Permanent Cessation of LIBOR

Number 4

Federal Reserve Board welcomes and supports release of proposal and supervisory statements that would enable clear end date for U.S. Dollar (USD) LIBOR and would promote the safety and soundness of the financial system

The Federal Reserve Board has welcomed and supported the release of a proposal and supervisory statements that would enable a clear end date for U.S. Dollar (USD) LIBOR and would promote the safety and soundness of the financial system.

The announcements today by regulators in the United States and United Kingdom and by the benchmark administrator for LIBOR together lay out a path forward in which banks should stop writing new USD LIBOR contracts by the end of 2021, while most legacy contracts will be able to mature before LIBOR stops.

"Today's plan ensures that the transition away from LIBOR will be orderly and fair for everyone—market participants, businesses, and consumers," said Vice Chair for Supervision Randal K. Quarles.

Under the proposal from LIBOR's administrator, ICE Benchmark Administration Limited (IBA) will consult in early December on its intention to cease the publication of the one week and two month USD LIBOR settings immediately following the LIBOR publication on December 31, 2021, and the remaining USD LIBOR settings immediately following the LIBOR publication on June 30, 2023.

LIBOR's regulator, the United Kingdom's Financial Conduct Authority (FCA), also issued a statement welcoming these developments.

The FCA indicated it will, in coordination with US authorities and relevant authorities in other jurisdictions, consider whether and, if so, how to most appropriately limit new use of USD LIBOR by supervised entities in the UK, consistent with the FCA's objectives of protecting consumers and market integrity.

Concurrently, the Federal Reserve Board, Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation released a statement explaining that the June 30, 2023 cessation date for which IBA is consulting would allow time for "legacy contracts"—USD LIBOR transactions executed before January 1, 2022—to mature.

The guidance further notes that entering into new USD-LIBOR-based contracts creates safety and soundness risks. Given that, the banking agencies encourage banks to stop entering into those new contracts by end-2021.

"These announcements represent critical steps in the effort to facilitate an orderly wind-down of USD LIBOR," said John Williams, President of the Federal Reserve Bank of New York, in his capacity as Co-Chair of the Financial Stability Board's Official Sector Steering Group. "They propose a clear picture of the future, to help support transition planning over the next year and beyond."

For the purposes of language adopted by the International Swaps and Derivatives Association, this statement should not be read as announcing that the LIBOR benchmark has ceased, or will cease, to be provided permanently or indefinitely or that it is not, or no longer will be, representative.

Number 5

EIOPA launches discussion paper on a methodology for integrating climate change in the standard formula

The European Insurance and Occupational Pensions Authority (EIOPA) published a discussion paper on a methodology for the potential inclusion of climate change in the Solvency II standard formula when calculating natural catastrophe underwriting risk.

You may visit:
https://www.eiopa.europa.eu/content/discussion-paper-methodology-potential-inclusion-climate-change-nat-cat-standard-formula_en

This discussion paper is a follow-up to EIOPA's Opinion on Sustainability within Solvency II issued in September last year, which concluded that there is a need to consider if and how climate change-related perils could be better captured in the Solvency II framework under the natural catastrophe risk submodule.

The frequency and severity of natural catastrophes is expected to increase due to climate change.

Improved climate projections provide evidence that weather extremes such as heat waves, heavy precipitation, droughts, top wind speeds and storm surges will rise in many European regions.

To ensure the financial resilience of (re)insurers covering natural catastrophes, the solvency capital requirements for natural catastrophe underwriting risk need to remain appropriate in light of climate change.

In line with that, EIOPA proposes different methodological steps and process changes to integrate climate change in the calculation of natural catastrophe risk and invites all interested stakeholders to provide comments by 26 February 2021.

Background and Context

1.1. Due to climate change, the frequency and severity of natural catastrophes is expected to increase.

Improved climate projections provide evidence that future climate change will increase climate-related extremes (e.g. heat waves, heavy precipitation,

droughts, top wind speeds and storm surges) in many European regions (EEA, 2017 & 2020).

1.2. Climate change could therefore impact all underwriting modules in the standard formula (SF) (Life, Health and Non-life Life).

1.3. In the case of life and health underwriting risk, climate change may impact the sub-modules mortality, longevity, catastrophe and disability/morbidity risk.

More extreme weather events, such as heatwaves, could for example lead to higher mortality rates that could result in higher claims in mortality or morbidity portfolios.

However, the effect climate change may have on life and health underwriting risks will depend on different factors such as the line of business (LoB).

Climate change could also have an effect on the health cat sub-module, especially on the pandemic risk, because it might be possible that diseases which affect only particular parts of the world could also spread in other parts of the world in the future (e.g. malaria, Dengue) (Watts, 2020).

1.4. In the case of non-life underwriting risk climate change may have an impact on the sub-module premium risk. Climate impacts already observed may be priced in the premiums because non-life premiums are generally adapted on an annual basis.

Data used by EIOPA for the calibration of the premium risk standard deviation can therefore be assumed to provide a current view of climate change. The non-life catastrophe risk sub-module is one of the central modules to be impacted by climate change.

This sub-module consists of three separate and independent submodules dealing with natural catastrophe risk, man-made catastrophe risk and other catastrophe events.

The following analysis focuses on the natural catastrophe (Nat Cat) module as climate change could lead to more frequent and severe events that could lead to higher insured losses of non-life insurers.
To read more:
https://www.eiopa.europa.eu/content/discussion-paper-methodology-potential-inclusion-climate-change-nat-cat-standard-formula_en

Number 6

Why Islamic finance has an important role to play in supporting the recovery from Covid – and how the Bank of England's new Alternative Liquidity Facility can help

Andrew Hauser, Executive Director for Markets of the Bank of England, at the Markets UK Islamic Finance Week 2020, London.

Introduction

It's a privilege to be with you today to talk about the Bank of England's work on Islamic finance – and to announce the launch date for our new Shari'ah compliant non-interest based deposit facility, the first such account from a Western central bank.

The facility, in which deposits from Islamic banks will be backed by a return-generating fund of high quality Shari'ah compliant assets, will further strengthen the United Kingdom's role as the leading international financial centre for Islamic finance outside the Muslim world.

But it also goes deeper – because the core principles of Islamic finance are strikingly well suited to responding to some of the biggest challenges we will all face in rebuilding our economy once Covid has passed.

Prioritising equity-like risk-sharing over debt. Factoring ethical and environmental considerations into investment decisions. And embracing innovative financial solutions beyond traditional banking.

And that lies four square within the Bank of England's mission to promote the good of the people of the United Kingdom, Muslim and non-Muslim alike.

Global growth in Islamic Finance

Islamic finance is a global success story, with assets of $2.4 trillion in 2019 (Table 1). That's 11% higher than a year earlier, and fully a third bigger than in 2015.

Table 1: Size and composition of Islamic Finance Services Industry ($bn, 2019)

Region	Banking Assets	*Şukūk* Outstanding	Islamic Funds' Assets	*Takāful* Contributions	Total	Share
GCC*	854.0	204.5	36.4	11.70	**1,106.6**	**45.4%**
South-East Asia	240.5	303.3	26.7	3.02	**573.5**	**23.5%**
Middle East and South Asia	584.3	19.1	16.5	11.36	**631.3**	**25.9%**
Africa	33.9	1.8	1.6	0.55	**37.9**	**1.6%**
Others	53.1	14.7	21.1	0.44	**89.3**	**3.7%**
Total	**1,765.8**	**543.4**	**102.3**	**27.07**	**2,438.6**	**100%**
Share	**72.4%**	**22.3%**	**4.2%**	**1.1%**	**100.0%**	

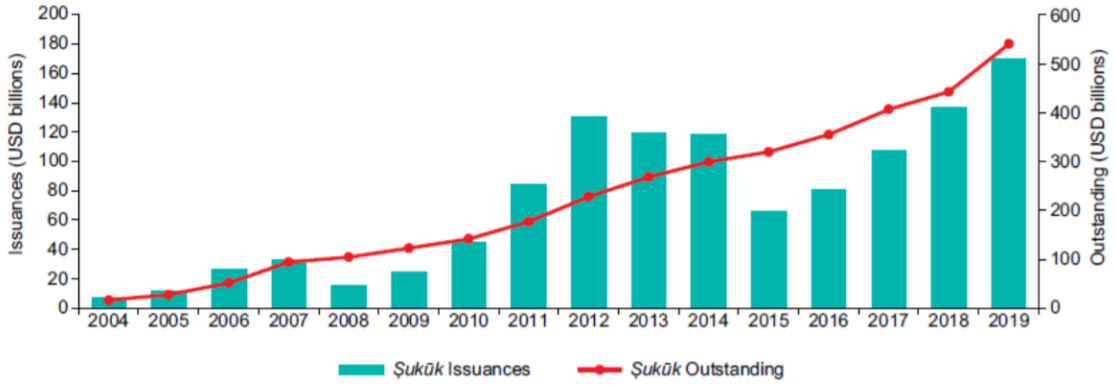
*Gulf Co-operation Council (Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates).

Source: Islamic Financial Services Industry Stability Report 2020[2]

Three quarters of those Islamic finance assets are held by banks – and are large enough to play a systemic role in thirteen countries.

There's also a nascent Islamic insurance industry (takaful) – and a much larger capital market, anchored around the growing stock of sukuk issued by companies and governments (Chart 1), and over 1,500 Shari'ah compliant investment funds.

Chart 1: Global sukuk issuance and stock outstanding



Source: Islamic Financial Services Industry Stability Report 2020[2]

The role of the UK and the Bank of England in supporting Islamic Finance

So far, so impressive. But what, you might ask, does all this have to do with the UK or the Bank of England, when the centre of gravity for Islamic finance lies in the Middle East, North Africa, South and South East Asia?

Well, the fact is that, outside those regions, the UK is the pre-eminent centre for Islamic finance. And that reflects its significant, well-established domestic Muslim population; its strong relationships with the wider Muslim world; and its deep expertise in financial market origination and

distribution, embedded in a mature legal and regulatory framework.

Indeed, Islamic finance in the UK goes back many decades: from commodity-based short term liquidity management and trade finance in the 1970s, to the first UK Islamic bank, investment funds and takaful in the early 1980s.

To read more:
https://www.bis.org/review/r201203a.pdf

Number 7

Advanced Persistent Threat Actors Targeting U.S. Think Tanks

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have observed persistent continued cyber intrusions by advanced persistent threat (APT) actors targeting U.S. think tanks.

This malicious activity is often, but not exclusively, directed at individuals and organizations that focus on international affairs or national security policy.

The following guidance may assist U.S. think tanks in developing network defense procedures to prevent or rapidly detect these attacks.

APT actors have relied on multiple avenues for initial access.

These have included low-effort capabilities such as spearphishing emails and third-party message services directed at both corporate and personal accounts, as well as exploiting vulnerable web-facing devices and remote connection capabilities.

Increased telework during the COVID-19 pandemic has expanded workforce reliance on remote connectivity, affording malicious actors more opportunities to exploit those connections and to blend in with increased traffic.

Attackers may leverage virtual private networks (VPNs) and other remote work tools to gain initial access or persistence on a victim's network.

When successful, these low-effort, high-reward approaches allow threat actors to steal sensitive information, acquire user credentials, and gain persistent access to victim networks.

Given the importance that think tanks can have in shaping U.S. policy, CISA and FBI urge individuals and organizations in the international affairs and national security sectors to immediately adopt a heightened state of awareness and implement the critical steps listed in the Mitigations section of this Advisory.

MITIGATIONS

CISA and FBI recommend think tank organizations apply the following critical practices to strengthen their security posture.
Leaders

• Implement a training program to familiarize users with identifying social engineering techniques and phishing emails.

Users/Staff

• Log off remote connections when not in use.

• Be vigilant against tailored spearphishing attacks targeting corporate and personal accounts (including both email and social media accounts).

• Use different passwords for corporate and personal accounts.

• Install antivirus software on personal devices to automatically scan and quarantine suspicious files.

• Employ strong multi-factor authentication for personal accounts, if available.

• Exercise caution when:

o Opening email attachments, even if the attachment is expected and the sender appears to be known.

o Using removable media (e.g., USB thumb drives, external drives, CDs).
IT Staff/Cybersecurity Personnel

• Segment and segregate networks and functions.

• Change the default username and password of applications and appliances.

• Employ strong multi-factor authentication for corporate accounts.

• Deploy antivirus software on organizational devices to automatically scan and quarantine suspicious files.

IT Staff/Cybersecurity Personnel

• Segment and segregate networks and functions.

• Change the default username and password of applications and appliances.

• Employ strong multi-factor authentication for corporate accounts.

• Deploy antivirus software on organizational devices to automatically scan and quarantine suspicious files.

• Apply encryption to data at rest and data in transit.

• Use email security appliances to scan and remove malicious email attachments or links.

• Monitor key internal security tools and identify anomalous behavior. Flag any known indicators of compromise or threat actor behaviors for immediate response.

• Organizations can implement mitigations of varying complexity and restrictiveness to reduce the risk posed by threat actors who use Tor (The Onion Router) to carry out malicious activities.

See the CISA-FBI Joint Cybersecurity Advisory on Defending Against Malicious Cyber Activity Originating from Tor for mitigation options and additional information.

• Prevent exploitation of known software vulnerabilities by routinely applying software patches and upgrades.

Foreign cyber threat actors continue to exploit publicly known—and often dated—software vulnerabilities against broad target sets, including public and private sector
organizations.

If these vulnerabilities are left unpatched, exploitation often requires few resources and provides threat actors with easy access to victim networks. Review CISA and FBI's Top 10 Routinely Exploited Vulnerabilities and other CISA alerts that identify vulnerabilities exploited by foreign attackers.

• Implement an antivirus program and a formalized patch management process.

• Block certain websites and email attachments commonly associated with malware (e.g., .scr, .pif, .cpl, .dll, .exe).

• Block email attachments that cannot be scanned by antivirus software (e.g., .zip files).

• Implement Group Policy Object and firewall rules.

• Implement filters at the email gateway and block suspicious IP addresses at the firewall.

• Routinely audit domain and local accounts as well as their permission levels to look for situations that could allow an adversary to gain wide access by obtaining credentials of a privileged account.

• Follow best practices for design and administration of the network to limit privileged account use across administrative tiers.

• Implement a Domain-Based Message Authentication, Reporting & Conformance (DMARC) validation system.

• Disable or block unnecessary remote services.

• Limit access to remote services through centrally managed concentrators.

• Deny direct remote access to internal systems or resources by using network proxies, gateways, and firewalls.

• Limit unnecessary lateral communications.

• Disable file and printer sharing services. If these services are required, use strong passwords or Active Directory authentication.

• Ensure applications do not store sensitive data or credentials insecurely.

• Enable a firewall on agency workstations, configured to deny unsolicited connection requests.

• Disable unnecessary services on agency workstations and servers.

• Scan for and remove suspicious email attachments; ensure any scanned attachment is its "true file type" (i.e., the extension matches the file header).

• Monitor users' web browsing habits; restrict access to suspicious or risky sites.

Contact law enforcement or CISA immediately regarding any unauthorized network access identified.

• Visit the MITRE ATT&CK techniques and tactics pages linked in the ATT&CK Profile section above for additional mitigation and detection strategies for this malicious activity targeting think tanks.

The paper:
https://us-cert.cisa.gov/sites/default/files/publications/AA20-336A-APT_Actors_Targeting_US_ThinkTanks.pdf

Number 8

Face Recognition Software Shows Improvement in Recognizing Masked Faces

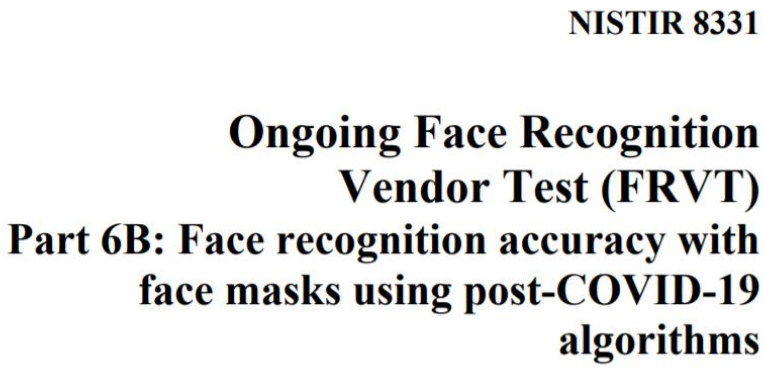
Latest NIST test is the first to measure performance of software submitted after pandemic's arrival.

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

A new study of face recognition technology created after the onset of the COVID-19 pandemic shows that some software developers have made demonstrable progress at recognizing masked faces.

The findings, produced by the National Institute of Standards and Technology (NIST), are detailed in a new report called Ongoing Face Recognition Vendor Test (FRVT) Part 6B: Face Recognition Accuracy with Face Masks Using Post-COVID-19 Algorithms (NISTIR 8331).
You may visit:
https://www.nist.gov/publications/ongoing-face-recognition-vendor-test-frvt-part-6b-face-recognition-accuracy-face-masks

https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8331.pdf


NISTIR 8331

Ongoing Face Recognition Vendor Test (FRVT)
Part 6B: Face recognition accuracy with face masks using post-COVID-19 algorithms

It is the agency's first study that measures the performance of face recognition algorithms developed following the arrival of the pandemic. A previous report from July explored the effect of masked faces on algorithms submitted before March 2020, indicating that software available before the pandemic often had more trouble with masked faces.

"Some newer algorithms from developers performed significantly better than their predecessors. In some cases, error rates decreased by as much as a factor of 10 between their pre- and post-COVID algorithms," said NIST's Mei Ngan, one of the study's authors. "In the best cases, software

algorithms are making errors between 2.4 and 5% of the time on masked faces, comparable to where the technology was in 2017 on nonmasked photos."

The new study adds the performance of 65 newly submitted algorithms to those that were tested on masked faces in the previous round, offering cumulative results for 152 total algorithms.

Developers submitted algorithms to the FRVT voluntarily, but their submissions do not indicate whether an algorithm is designed to handle face masks, or whether it is used in commercial products.

Using the same set of 6.2 million images as it had previously, the team again tested the algorithms' ability to perform "one-to-one" matching, in which a photo is compared with a different photo of the same person — a function commonly used to unlock a smartphone. (The team did not test algorithms' ability to perform "one-to-many" matching — often used to find matches in a large database — but plans to do so in a later round.) And as with the July report, the images had mask shapes digitally applied, rather than showing people wearing actual masks.

Some of the report's findings include:

When both the new image and the stored image are of masked faces, error rates run higher. With a couple of notable exceptions, when the face was occluded in both photos, false match rates ran 10 to 100 times higher than if the original saved image showed an uncovered face. Smartphones often use one-to-one matching for security, and it would be far more likely for a stranger to successfully unlock a phone if the saved image was of a masked person.

The more of a face a mask covers, the higher the algorithm's error rate tends to be. Continuing a trend from the July 2020 report, round mask shapes — which cover only the mouth and nose — generated fewer errors than wide ones that stretch across the cheeks, and those covering the nose generated more errors than those that did not.

Mask colors affect the error rate. The new study explored the effects of two new mask colors — red and white — as well as the black and light blue masks the July study tested. While there were exceptions, the red and black masks tended to yield higher error rates than the other colors did. The research team did not investigate potential reasons for this effect.

A few algorithms perform well with any combination of masked or unmasked faces. Some developers have created "mask-agnostic" software

that can handle images regardless of whether or not the faces are masked. The algorithms detect the difference automatically, without being told.

A final significant point that the NIST research team makes also carries over from previous studies: Individual algorithms differ. End users need to get to know how their chosen software performs in their own specific situations, ideally using real physical masks rather than the digital simulations the team used in the study.

“It is incumbent upon the system owners to know their algorithm and their data,” Ngan said. “It will usually be informative to specifically measure accuracy of the particular algorithm on the operational image data collected with actual masks.”

Number 9

K9 Chemistry: A Safer Way to Train Detection Dogs

Canine trainers may no longer need to handle or expose dogs to real explosives and narcotics.

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

Trained dogs are incredible chemical sensors, far better at detecting explosives, narcotics and other substances than even the most advanced technological device. But one challenge is that dogs have to be trained, and training them with real hazardous substances can be inconvenient and dangerous.

NIST scientists have been working to solve this problem using a jello-like material called polydimethylsiloxane, or PDMS for short. PDMS absorbs odors and releases them slowly over time.

Enclose it in a container with an explosive or narcotic for a few weeks until it absorbs the odors, and you can then use it to safely train dogs to detect the real thing.

But a few weeks is a long time, and now, NIST researchers have developed a faster way to infuse PDMS with vapors. In the journal Forensic Chemistry, they describe warming compounds found in explosives, causing them to release vapors more quickly, then capturing those vapors with PDMS that is maintained at a cooler temperature, which allows it to absorb vapors more readily.

This two-temperature method cut the time it took to “charge” PDMS training aids from a few weeks to a few days.

“That time savings can be critical,” said NIST research chemist Bill MacCrehan. “If terrorists are using a new type of explosive, you don’t want to wait a month for the training aids to be ready.”

For this experiment, MacCrehan infused PDMS with vapors from dinitrotoluene (DNT), which is a low-level contaminant present in TNT explosives but the main odorant that dogs respond to when detecting TNT.

He also infused PDMS with vapors from a small quantity of TNT. Co-authors at the Auburn University College of Veterinary Medicine then demonstrated that trained detection dogs responded to the DNT-infused PDMS training aids as if they were real TNT.

While this study focused on DNT as a proof of concept, MacCrehan says he believes the two-temperature method will also work with other explosives and with narcotics such as fentanyl.

Some forms of fentanyl are so potent that inhaling a small amount can be harmful or fatal to humans and dogs. But by controlling how much vapor the PDMS absorbs, MacCrehan says, it should be possible to create safe training aids for fentanyl.

Other safe training aids already exist. Some are prepared by dissolving explosives and applying the solution to glass beads, for example. “But most have not been widely accepted in the canine detection community because their effectiveness has not been proven,” said Paul Waggoner, a co-author and co-director of Auburn’s Canine Performance Sciences Program. “If you put an explosive in a solvent, the dogs might actually be detecting the solvent, not the explosive.”

To test the two-temperature method, MacCrehan devised a PDMS “charging station” with a hot plate on one side and a cooling plate on the other (so the “hot stays hot and the cool stays cool,” as a 1980s commercial jingle put it).

He prepared various samples by placing the DNT on the hot side, where the chemical was warmed to temperatures ranging from 30 to 35 degrees Celsius (86 to 95 degrees Fahrenheit) — well below the temperature that would cause TNT to detonate.

The PDMS was kept a relatively cool 20 degrees Celsius, or about room temperature, on the other side of the charging station.

MacCrehan loaded the DNT-infused PDMS samples, which hold their charge for up to a few months, into perforated metal cans. He also loaded several cans with blanks — PDMS samples to which no vapors were added. He labeled the cans with codes and shipped them to Auburn University.

The researchers at Auburn had trained a team of six Labrador retrievers to detect TNT using real TNT explosives. They then conducted a study to determine if the dogs would alert to the PDMS from NIST samples as if it were real TNT.

This study was “double blind”: Neither the dog handlers nor the note-takers who scored the dogs’ responses knew which containers underwent which preparation. This is important because dogs are keenly attuned to the body language of their handlers.

If the handlers knew which samples were prepared with DNT, they might inadvertently cue the dogs with the direction of their gaze, a subtle shift in body position or some other subconscious gesture. And if the note-takers knew which samples were which, they might over-interpret the dogs' responses.

The dogs alerted to all the DNT-infused PDMS samples. They did not alert to the blanks, meaning that they were responding to the DNT, not to the PDMS itself. "They responded to the samples as if they were the real thing," Waggoner said.

The dogs did not respond as consistently to PDMS that was infused with limited quantities of TNT. However, MacCrehan explains that the very small amounts of TNT he used for this purpose may not have contained sufficient amounts of DNT to fully infuse the samples.

Looking forward, MacCrehan will be experimenting with ways to safely prepare PDMS training aids for the improvised explosives TATP and HMTD. These compounds are extremely unstable and detonate easily, so having safe training aids for them will be especially useful.

MacCrehan is a laboratory chemist, not an animal behavior expert. But despite his technological orientation, he is amazed by dogs. He estimates that they are 10,000 to 100,000 times more sensitive than the most sophisticated analytical instruments. "We are nowhere near having a hand-held gizmo that can do what they do," he said.

Number 10

DARPA Looks to Light up Integrated Photonics with Chip-Scale Laser Development

First demonstrated sixty years ago, the laser has become an essential technology in today's world. It has transformed diverse fields including communications, sensing, manufacturing, and medicine.

More recently, innovations in integrated photonics have allowed the miniaturization of key optical components and the ability to arrange several elements on a single silicon chip.

When combined with lasers, these photonic integrated circuits (PICs) have the potential to replace large and costly optical systems with chip-scale solutions.

However, due to differences in the properties of the materials that compose them, lasers and PICs are difficult to combine onto the same platform, limiting the benefits of integration and preventing broad technology impact.

To address this challenge, DARPA developed the Lasers for Universal Microscale Optical Systems (LUMOS) program, which aims to bring high-performance lasers to advanced photonics platforms.

As highlighted in the recent program kick-off meeting, LUMOS will address several commercial and defense applications by directing efforts across three distinct Technical Areas.

The first LUMOS Technical Area brings high-performance lasers and optical amplifiers into advanced domestic photonics manufacturing foundries.

Two research teams were selected in this area: Tower Semiconductor and SUNY Polytechnic Institute. These performers will work to demonstrate flexible, efficient on-chip optical gain in their photonics processes to enable next-generation optical microsystems for communications, computing, and sensing. LUMOS technologies will be made available to future design teams through DARPA-sponsored multi-project wafer runs.

The second LUMOS Technical Area seeks to develop high power lasers and amplifiers on fast photonics platforms for microwave applications.

Research teams include Ultra-Low Loss Technologies, Quintessent, Harvard University, and Sandia National Laboratories.

The final LUMOS Technical Area creates precise lasers and integrated photonic circuits for visible spectrum applications with an ambitious goal of "wavelength by design" across an unprecedented spectral range.

The teams will seek to develop lasers at many challenging wavelengths throughout the program to enable compact atomic sensors for navigation, precise timing solutions, and emerging quantum information hardware.

Selected research teams include Nexus Photonics, Yale University, California Institute of Technology, Sandia National Laboratories, and the University of Colorado at Boulder.

"LUMOS is part of the third phase of DARPA's Electronics Resurgence Initiative (ERI) – a five-year, upwards of $1.5 billion investment in the future of domestic, U.S. government, and defense electronics systems," said Gordon Keeler, program manager in DARPA's Microsystems Technology Office.

"As an ERI program, LUMOS aims to create unique, differentiated domestic manufacturing capabilities that are accessible to the DoD through the enhanced capabilities of existing foundries and through DoD-relevant demonstration systems created by the program performers."

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.

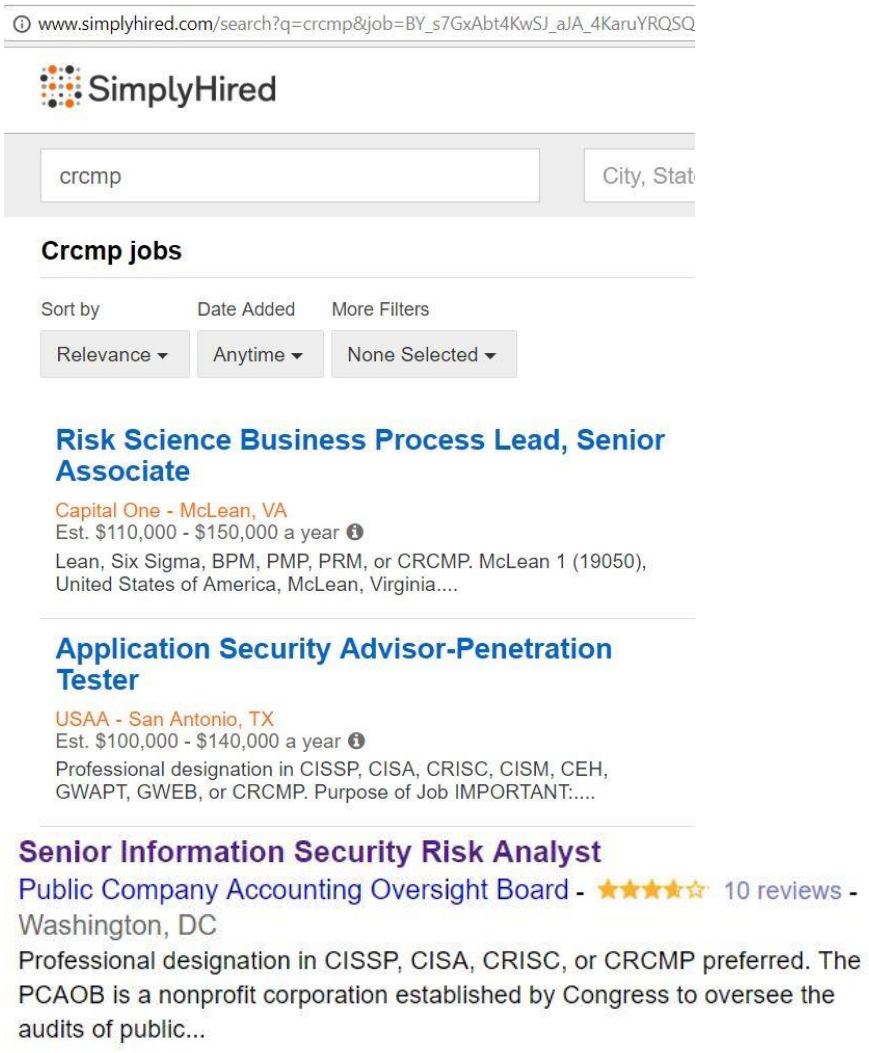
International Association of Risk and Compliance Professionals

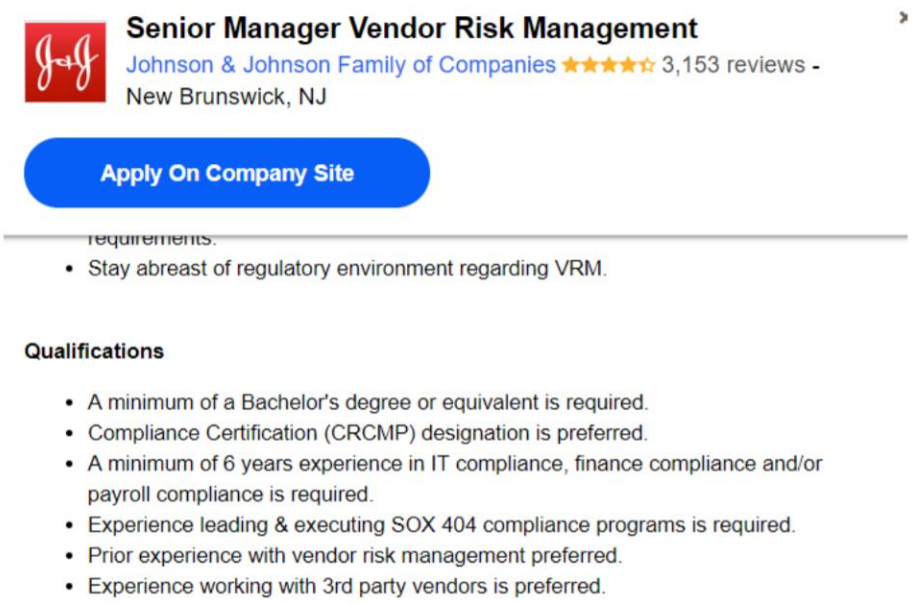
You can explore what we offer to our members:

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