Monday, June 15, 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,

T. S. Eliot believed that *humankind cannot bear very much reality*. But the Financial Stability Board (FSB) is probably following the advice of *Marcus Tullius Cicero:* If we are not ashamed to think it, we should not be ashamed to say it.

According to the FSB, the COVID-19 pandemic represents the biggest test of the post-crisis financial system to date. The pandemic constitutes an unprecedented global *macro-economic shock*, pushing the global economy into a recession of uncertain magnitude and duration.

The global financial system faces the dual challenge to sustain the flow of credit amidst declining growth and to manage heightened risks.

The FSB provided its assessment of financial stability risks related to COVID-19 in a report submitted to the 15 April 2020 virtual meeting of G20 Finance Ministers and Central Bank Governors.

According to this report, this exogenous shock has placed the financial system under strain. Downward revisions of expected economic activity and heightened risk aversion have led to a major re-pricing and repositioning in global financial markets.

On the one hand, the providers of funding have an increasing preference for short-term safe assets. On the other hand, *credit risks are rising sharply*. As a consequence, the demands on the financial system's capital and liquidity have risen. Heightened *operational risks* are adding to vulnerabilities.

The global financial system is more resilient and better placed to sustain

financing to the real economy as a result of the G20 regulatory reforms in the aftermath of the 2008 global financial crisis.

In particular, greater resilience of major banks at the core of the financial system has allowed the system to date largely to absorb rather than amplify the current macroeconomic shock. Those forms of market-based finance that contributed to the 2008 financial crisis pose significantly lower financial stability risks.

Financial market infrastructures, particularly CCPs, have functioned well, despite the challenging external financial and operational conditions. Nevertheless, given the unprecedented scale of the shock, key funding markets experienced acute stress and authorities needed to take a wide range of measures to sustain the supply of credit to the real economy and to support financial intermediation.

The FSB is examining the potential financial stability risks that may lie ahead as the impact of COVID-19 on the global economy unfolds. Going forward, the FSB intends to monitor the resilience of the critical nodes discussed in the G20 report on a frequent basis, so as to identify any emerging issues in a timely manner.

It also intends to identify and assess in a forward-looking manner the specific vulnerabilities that *may materialise* during this major global economic downturn, including potential sources of procyclicality.

Welcome to the Top 10 list.

Best regards,

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

Number 1 (Page 5)

Countering Covid-19: The nature of central banks' policy response

Agustín Carstens, General Manager of the BIS, at the UBS High-level Discussion on the Economic and Monetary Policy Outlook, Zurich.

Number 2 (Page 9)

Seven Moments in Spring: Covid-19, financial markets and the Bank of England's balance sheet operations

Andrew Hauser, Executive Director, Markets - Bloomberg, London

BANK OF ENGLAND

Number 3 (Page 11)

Top ten cyber hygiene tips for SMEs during covid-19 pandemic

The EU Agency for Cybersecurity releases ten cyber hygiene tips to support SMEs in protecting their virtual assets against cyber-attacks, during the COVID-19 pandemic.

enisa
European Network and Information Security Agency

Number 4 (Page 13)

PCAOB Issues Six Largest U.S. Firm Inspection Reports in New User-Friendly Format, Guide to Reading Reports

PCAOB
Public Company Accounting Oversight Board

Number 5 (Page 15)

Central banks' response to Covid-19 in advanced economies

Paolo Cavallino and Fiorella De Fiore

BIS

Number 6 (Page 18)

Executive Order on Preventing Online Censorship

Number 7 (Page 25)

Oregon FBI Tech Tuesday: Building a Digital Defense by Recognizing Signs of Trouble

Number 8 (Page 27)

Preparing for Cyberattacks and Technical Problems During the Pandemic: A Guide for Election Officials

BRENNAN CENTER FOR JUSTICE

Number 9 (Page 30)

Multiple Vulnerabilities identified by Cisco in their ASA and FTD software and routers

Number 10 (Page 32)

NIST Seeks Public Input on Use of Positioning, Navigation and Timing Services

Agency plans guidance to strengthen cybersecurity of related tech, in response to White House order.

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

Number 1

Countering Covid-19: The nature of central banks' policy response

Agustín Carstens, General Manager of the BIS, at the UBS High-level Discussion on the Economic and Monetary Policy Outlook, Zurich.

It is a pleasure and an honour to participate in this panel with Thomas Jordan and Axel Weber. Axel, thank you very much for the invitation.

I join Thomas in expressing my sympathy to everyone who has been affected by this pandemic and wishing all of you in the audience good health. In my opening remarks, I will briefly address the economic impact of Covid-19, to then move on to analyse the policy response of primarily the advanced economies' central banks.

No normal recession

The Covid-19 pandemic and the induced global lockdown are a truly historic event. Never before has the global economy been deliberately put into an induced coma. This is no normal recession, but one that results from explicit policy choices to avoid a large-scale public health disaster.

The unique character of this recession poses unfamiliar challenges. On the demand side, lockdowns and social distancing have made consumer spending highly insensitive to policy stimulus.

On the supply side, containment measures ordered by governments have directly hindered production, with the repercussions spreading through local and global supply chains. These disruptions could leave permanent scars on the economy if they result in large-scale layoffs and bankruptcies.

The pandemic also profoundly shook financial markets. As events unfolded, heavy sell-offs across a wide range of assets and a sharp tightening of financial conditions threatened to derail the economy even further.

The policy reaction has been unprecedented. Governments, central banks and supervisory authorities have responded boldly, decisively and imaginatively to limit the consequences of simultaneous sudden stops in spending, economic activity, funding and financial market functioning.

In particular, it took massive and unprecedented policy actions on the part of central banks and other authorities to prevent a financial collapse that would have compounded the drop in real activity.

On the fiscal side, governments have launched massive stimulus and projected fiscal deficits on a scale not seen since World War II.

A major issue will be how to finance the resulting fiscal deficits and prevent them from destabilising markets. In addition, the fiscal measures have been accompanied by far-reaching funding and credit guarantees provided by governments and/or their development banks.

The response of central banks

The sudden shock called for a speedy and massive policy response .The actions of central banks have again highlighted their central role in crisis management as they swiftly cut policy interest rates and launched large-scale balance sheet measures

This brought central banks to the forefront again as they can mobilise financial resources faster than any other authority. In this round of urgent policy mobilisation, central banks' actions concentrated on large-scale purchases of government debt as well as credit support for firms and households.

The latter encompassed funding-for lending schemes, purchases of corporate debt, and support provisions for small and medium-sized enterprises. This last set of measures is designed to travel the "last mile".

The main objective is to prevent liquidity strains that could lead to bankruptcies of solvent firms and leave long-lasting scars on growth potential. These extraordinary actions were designed precisely to flatten the mortality curve of businesses.

For their part, large-scale government bond purchases aim to lower interest rates, to provide monetary stimulus and to help the liquidity and functioning of the sovereign bond markets. This comes in the context of huge borrowing needs by governments as fiscal deficits rise and debt levels surge.

The last feature reflects the rarely employed role of the central bank as a market stabiliser and financing intermediary between the fiscal authorities and financial markets.

This should be temporary, limited by its intent and scale, and in line with the financial stability mandate of central banks. These actions are meant to smooth the impact of a sudden ramp-up of fiscal spending induced by an extraordinary but, we hope, transient event.

These extraordinary monetary policy actions are designed exclusively to safeguard economic and financial stability, and do not amount to fiscal deficit financing. Consistent with this, the measures undertaken by central banks have contributed to an easing of financial conditions and a calming of financial turmoil.

Setting the boundaries

We could conceptualize the life cycle of a pandemic-induced crisis as having three phases: liquidity, solvency and recovery.

In many countries, we are at the end of the first stage, or at the end of the beginning, where monetary policy actions can be most effective. For the later phases, the heavy lifting should come primarily from fiscal and structural policies.

While central bank measures have been necessary and show initial success, these bring major challenges going forward in the form of a significant overlap between fiscal and monetary policy.

Central bank balance sheets are bound to grow considerably this year, in tandem with a massive increase in public debt. There is a growing nexus between fiscal and monetary policies. Against this background, how can we safeguard central bank independence and credibility going forward?

First, fiscal sustainability should be assured, otherwise perceptions may arise that debt could be inflated away. Governments can start by crafting strong intertemporal fiscal strategies, reining in future spending and developing sound revenue policies.

But the most direct route to fiscal sustainability lies in boosting growth potential. This means implementing structural reforms to lift potential growth rates, mitigating failures of healthy firms, orienting fiscal policies towards investment, preserving global supply chains and safeguarding free trade .

Second, central bank policies need to remain credibly focused on maintaining macroeconomic stability. Actions should remain in line with mandates, particularly price and financial stability.

The intention behind policy actions should be clearly articulated and overt deficit financing avoided. Proper, institutional governance should be preserved.

Wherever possible, indemnities of governments to cover potential central bank losses are extremely useful. Exit strategies should be articulated as soon as possible. Of course, an optimal exit is one that is induced by a favourable economic environment.

The bottom line is that there is a need to recognise the limits of monetary policy. Central banks cannot intervene in government debt markets on a large scale for any great length of time. Eventually, the natural boundaries between fiscal and monetary policy will need to be fully restored to preserve central bank credibility.

Finally, let me say that the aggressive measures described, crossing the traditional boundaries between fiscal and monetary policies, are only feasible for central banks in advanced economies with high credibility stemming from a long track record of stability-oriented policies. This is strong medicine and should only be taken with extreme care.

Number 2

Seven Moments in Spring: Covid-19, financial markets and the Bank of England's balance sheet operations

Andrew Hauser, Executive Director, Markets - Bloomberg, London

BANK OF ENGLAND

I have always had a funny feeling about Friday the 13th – and 13 March 2020, Mark Carney's last day in the office as Governor of the Bank of England, was no exception.

Two days earlier, on Wednesday 11 March, the Bank and HM Treasury had launched an unprecedentedly comprehensive package of measures to respond to the rapidly growing economic consequences of the spread of Covid-19.

Hailed globally as a shining example of how monetary, fiscal and regulatory policies could work together to reinforce one another, the combination of interest rate cuts, government spending, cheap funding and capital easing measures seemed sure to stabilise markets and restore some much needed confidence to households and businesses.

So it cannot have been hugely welcome when, on Friday morning, with the removal vans waiting outside, I suggested the Bank's Governors needed to meet again before the weekend.

The previous day had seen disorderly conditions in the US Treasury market and the largest one-day fall in equity prices since the 1987 crash, despite major new policy announcements from the Federal Reserve and ECB.

As I ran through my gloomy update, it was clear that further action would be needed – but perhaps not at that stage quite how much more. Monday morning would be no quiet start for Andrew Bailey, the new Governor.

In my remarks today, I want to give a bird's eye's view of what happened in those extraordinary weeks, and the steps we took – either in concert with others, or using our own balance sheet – to neutralise the sudden pre-lockdown 'dash for cash' – the biggest test of core market functioning and resilience since the Great Financial Crisis (GFC) of 2008-9.

Judged solely against that narrow yardstick, central bank actions – unprecedented in scale and speed – were successful in averting a market meltdown. Commercial banks, strengthened by the post-GFC reforms, have continued to lend, supported by a range of public sector schemes. And we

learned some surprisingly positive things about operating a financial system remotely – both in terms of market resilience, but also in terms of diversity and inclusion.

But this is no time for self-congratulation. The broader aspects of the Covid-19 crisis – medical, social, economic, and personal – remain hugely challenging, and involve a much wider set of actors than central banks alone.

Further financial instability cannot be ruled out. And the sheer scale of the balance sheet interventions necessary in recent months pose important longer term questions. About the extent to which the non-bank financial system may still be capable of amplifying instability – for example through sudden non-bank deleveraging, runs on money market funds, or rigidities in dealer intermediation.

And about the appropriate balance of responsibilities between the public and private sector for dealing with such vulnerabilities.

I cannot give comprehensive answers to these questions today. But, in what follows, I have tried to provide some raw material for that exercise, illustrated using seven of the most vivid 'moments' from my own experience of the past few weeks.

To read more:
https://www.bankofengland.co.uk/-/media/boe/files/speech/2020/seven-moments-in-spring-covid-19-speech-by-andrew-hauser.pdf

Number 3

Top ten cyber hygiene tips for SMEs during covid-19 pandemic

The EU Agency for Cybersecurity releases ten cyber hygiene tips to support SMEs in protecting their virtual assets against cyber-attacks, during the COVID-19 pandemic.

Crises like the current COVID-19 pandemic have a serious impact on the European as well as the International society and economy. Small and medium-sized enterprises (SMEs) are often coping with difficult times. Unfortunately, cybercriminals often see such crises as opportunities. Phishing and ransomware attacks are on the rise.

SMEs are also faced with a new reality where employees are working more from home. This way they become even more dependent on Information Technology (IT) than before.

It goes without saying that protecting these virtual assets is of utmost importance to almost every SME. According to ENISA, the top ten cyber hygiene topics that SMEs should address, possibly through outsourcing where needed, are presented below:

1. Management buy-in. It is important that management sees the importance of cybersecurity for the organisation and that it is informed on a regular basis.

2. Risk assessment. This answers the question: what do I have to protect and from what? Identify and prioritise the main assets and threats your organisation is facing.

3. Cybersecurity policy. Have the necessary policies in place to deal with cybersecurity and appoint someone, for example an Information Security Officer (ISO), who is responsible for overseeing the implementation of these policies.

4. Awareness. Employees should understand the risks and should be informed about how to behave online. People tend to forget such things rather rapidly, so repeating this every now and then can be valuable.

5. Updates. Keeping everything, meaning servers, workstations, smartphones, etc. up-to-date is key in your cyber hygiene. Applying security

updates is part of this process. Ideally, this whole process is to a certain level automated and the updates can be tested in a testing environment.

6. Backups. Prior to doing these updates it is vital to have good backups in place. This will also protect the environment from attacks such as ransomware.

Backup the most important data often and think about the cost of losing data during a certain timespan. Keep the backups offline, test the backups and try to have duplication of the backups.

7. Access management. Have rules/policies in place for access management and enforce them. Make sure default passwords are changed for example, that passwords are not shared, etc.

8. Endpoint protection. Think about securing the endpoints through for example installing antivirus software.

9. Secure remote access. Limit remote access as much as possible and where absolutely needed, enable it but in a secure way. Make sure that communication is encrypted properly.

10. Incident management plan. There should be a plan on how to handle an incident when it occurs. Different realistic scenarios could be part of this plan. Get to know whom you could contact when things are problematic, for instance the national CSIRT.

Number 4

PCAOB Issues Six Largest U.S. Firm Inspection Reports in New User-Friendly Format, Guide to Reading Reports

PCAOB
Public Company Accounting Oversight Board

The Public Company Accounting Oversight Board (PCAOB) today issued the 2018 inspection reports for the six largest U.S. audit firms in a new, redesigned format.

The new format marks the first time the PCAOB has substantially changed its reports since the Board first issued a report more than fifteen years ago.

"One of the Board's top strategic priorities over the past two years has been to communicate more effectively with investors, audit committees, and other key stakeholders," said Chairman William D. Duhnke III.

"Our inspection reports are one of the primary ways we communicate with the public about our oversight activities, and we have heard time and again through our external engagement that the reports can be improved. We are pleased to share our new report with the public, and look forward to hearing feedback."

The PCAOB's new inspection report format streamlines the report's content to enhance readability and utilizes new charts and graphs to make the information more digestible and accessible for users.

It also includes new information not previously communicated in inspection reports to enhance transparency, which is one of the Board's strategic goals.

To further detail the key changes to the report and assist stakeholders in reading it, the PCAOB has issued a Guide to Reading the PCAOB's New Inspection Report.PDF This guide also solicits public feedback on our new report format.

In addition to the six reports issued today, reports for other annually inspected firms will adhere to this new format.

All triennially inspected firms' reports, beginning with the 2019 inspection reports, will utilize a similar format, but may not include all of the same data as the annually inspected firms' reports due to the frequency of our inspections and the size and nature of those firms.

BDO USA, LLP. You may visit:
https://pcaobus.org/Inspections/Reports/Documents/104-2020-007-BDO-USA-LLP.pdf

Deloitte & Touche LLP. You may visit:
https://pcaobus.org/Inspections/Reports/Documents/104-2020-008-Deloitte-Touche-LLP.pdf

Ernst & Young LLP. You may visit:
https://pcaobus.org/Inspections/Reports/Documents/104-2020-009-Ernst-Young-LLP.pdf

Grant Thornton LLP. You may visit:
https://pcaobus.org/Inspections/Reports/Documents/104-2020-010-Grant-Thornton-LLP.pdf

KPMG LLP. You may visit:
https://pcaobus.org/Inspections/Reports/Documents/104-2020-011-KPMG-LLP.pdf

PricewaterhouseCoopers LLP. You may visit:
https://pcaobus.org/Inspections/Reports/Documents/104-2020-012-PricewaterhouseCoopers-LLP.pdf

Number 5

Central banks' response to Covid-19 in advanced economies

Paolo Cavallino and Fiorella De Fiore

BIS

Key takeaways

- Central banks in advanced economies reacted swiftly and forcefully to the Covid-19 pandemic, deploying the full range of crisis tools within weeks.

  The initial response focused primarily on easing financial stress and ensuring a smooth flow of credit to the private non-financial sector.

- The pandemic triggered complementary responses from monetary and fiscal authorities.

  Fiscal backstops and loan guarantees supported central bank actions. Asset purchases, designed to achieve central banks' objectives, helped contain the costs of fiscal expansions.

- The footprint of central banks' measures will be sizeable. Across the five largest advanced economies, balance sheets are projected to grow on average by 15–23% of GDP before end2020 and to remain large in the near future.

The outbreak of Covid-19 was a shock of unprecedented size and nature. Lockdowns and containment measures on a global scale led to a generalised sudden stop in economic activity.

Workers' reduced income – particularly for precarious workers – exacerbated the fall in demand induced by distancing measures and contributed to an increase in the risk of delinquency on mortgages and consumer loans.

Businesses suffered from collapsing productive activities and reduced cash flow, which was particularly acute in sectors such as automotive, retail and travel. Concerns about household and corporate liquidity, combined with heightened uncertainty, hampered the functioning of key financial market segments.

In March 2020, corporate spreads surged globally for high-yield as well as investment grade issuers.

The markets for asset-backed and mortgage-backed securities froze in many countries. Commercial paper markets experienced strain in the United States, Canada and the euro area due to enhanced rollover risk.

Equity markets came under stress, and implied volatilities jumped for a wide range of assets. The global dash-for-cash disrupted fixed income asset markets.

The US Treasury market experienced a sharp sell-off leading to spikes in long-term yields (Schrimpf, Shin and Sushko (2020)). Pressures arose in the Japanese government bond (JGB) market, and sovereign spreads widened substantially in the euro area.

Central banks responded promptly and forcefully, consistent with their mandates, to preserve smooth market functioning and an effective transmission of monetary policy.

This Bulletin reviews the response of the central banks of the United States, the euro area, Japan, the United Kingdom and Canada.

A swift and forceful reaction

The overriding goal of central banks was to cushion the inevitable drop in economic activity by ensuring a smooth functioning of the financial system and facilitating the flow of credit to households and firms.

In doing so, central banks performed their traditional crisis role as lenders of last resort to the financial sector. They extended it further to become providers of liquidity to the private non-financial sector.

Central banks' response — Table 1

		Bank of Canada	Bank of England	Bank of Japan	Eurosystem	US Federal Reserve System
Interest rate		–1.5%	–0.65%			–1.50%
Lending operations	short-term	TROs, STLF, CTRF	CTRF, W&MF	FSOs, ROs, SLF	LTROs	ROs, PDCF, MMLF
	long-term	TROs	TFSME	SOCF, SOSME	TLTRO III, PELTROs	TALF, MSLP. PPPLF
Asset purchases	short-term	BAPF, PMMP, CPPP	CCFF	CPPs	APP, PEPP	CPFF, MLF
	long-term	CMBP, GCSPs, PBPP, CBPP	APF	JGBPs, CBPs, ETFPs, JREITPs	APP, PEPP	SOMA, PMCCF, SMCCF
Foreign exchange				YEN SL	EUR SLs	USD SLs, FIMA RF

See tables in online appendix for definition of acronyms. In some jurisdictions, central banks have macroprudential and supervisory roles, and can additionally adjust regulation. This taxonomy comprises only monetary measures.

Source: Central bank websites.

Between March and April 2020, the five central banks under review deployed the full set of crisis management policies at their disposal (Table 1). They all offered new lending operations, and either extended or inaugurated asset purchase programmes.

The Federal Reserve, the Bank of Canada and the Bank of England also cut interest rates. In addition, the Federal Reserve and, on a lesser scale, the ECB and the Bank of Japan increased the availability of their currencies abroad through swap lines.

To read more: https://www.bis.org/publ/bisbull21.pdf

Number 6

Executive Order on Preventing Online Censorship

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. Free speech is the bedrock of American democracy. Our Founding Fathers protected this sacred right with the First Amendment to the Constitution. The freedom to express and debate ideas is the foundation for all of our rights as a free people.

In a country that has long cherished the freedom of expression, we cannot allow a limited number of online platforms to hand pick the speech that Americans may access and convey on the internet. This practice is fundamentally un-American and anti-democratic. When large, powerful social media companies censor opinions with which they disagree, they exercise a dangerous power. They cease functioning as passive bulletin boards, and ought to be viewed and treated as content creators.

The growth of online platforms in recent years raises important questions about applying the ideals of the First Amendment to modern communications technology. Today, many Americans follow the news, stay in touch with friends and family, and share their views on current events through social media and other online platforms. As a result, these platforms function in many ways as a 21st century equivalent of the public square.

Twitter, Facebook, Instagram, and YouTube wield immense, if not unprecedented, power to shape the interpretation of public events; to censor, delete, or disappear information; and to control what people see or do not see.

As President, I have made clear my commitment to free and open debate on the internet. Such debate is just as important online as it is in our universities, our town halls, and our homes. It is essential to sustaining our democracy.

Online platforms are engaging in selective censorship that is harming our national discourse. Tens of thousands of Americans have reported, among other troubling behaviors, online platforms “flagging” content as inappropriate, even though it does not violate any stated terms of service;

making unannounced and unexplained changes to company policies that have the effect of disfavoring certain viewpoints; and deleting content and entire accounts with no warning, no rationale, and no recourse.

Twitter now selectively decides to place a warning label on certain tweets in a manner that clearly reflects political bias. As has been reported, Twitter seems never to have placed such a label on another politician's tweet. As recently as last week, Representative Adam Schiff was continuing to mislead his followers by peddling the long-disproved Russian Collusion Hoax, and Twitter did not flag those tweets. Unsurprisingly, its officer in charge of so-called 'Site Integrity' has flaunted his political bias in his own tweets.

At the same time online platforms are invoking inconsistent, irrational, and groundless justifications to censor or otherwise restrict Americans' speech here at home, several online platforms are profiting from and promoting the aggression and disinformation spread by foreign governments like China. One United States company, for example, created a search engine for the Chinese Communist Party that would have blacklisted searches for "human rights," hid data unfavorable to the Chinese Communist Party, and tracked users determined appropriate for surveillance. It also established research partnerships in China that provide direct benefits to the Chinese military.

Other companies have accepted advertisements paid for by the Chinese government that spread false information about China's mass imprisonment of religious minorities, thereby enabling these abuses of human rights. They have also amplified China's propaganda abroad, including by allowing Chinese government officials to use their platforms to spread misinformation regarding the origins of the COVID-19 pandemic, and to undermine pro-democracy protests in Hong Kong.

As a Nation, we must foster and protect diverse viewpoints in today's digital communications environment where all Americans can and should have a voice. We must seek transparency and accountability from online platforms, and encourage standards and tools to protect and preserve the integrity and openness of American discourse and freedom of expression.

Sec. 2. Protections Against Online Censorship. (a) It is the policy of the United States to foster clear ground rules promoting free and open debate on the internet. Prominent among the ground rules governing that debate is the immunity from liability created by section 230(c) of the Communications Decency Act (section 230(c)). 47 U.S.C. 230(c). It is the policy of the United States that the scope of that immunity should be clarified: the immunity should not extend beyond its text and purpose to

provide protection for those who purport to provide users a forum for free and open speech, but in reality use their power over a vital means of communication to engage in deceptive or pretextual actions stifling free and open debate by censoring certain viewpoints.

Section 230(c) was designed to address early court decisions holding that, if an online platform restricted access to some content posted by others, it would thereby become a "publisher" of all the content posted on its site for purposes of torts such as defamation. As the title of section 230(c) makes clear, the provision provides limited liability "protection" to a provider of an interactive computer service (such as an online platform) that engages in "'Good Samaritan' blocking" of harmful content.

In particular, the Congress sought to provide protections for online platforms that attempted to protect minors from harmful content and intended to ensure that such providers would not be discouraged from taking down harmful material. The provision was also intended to further the express vision of the Congress that the internet is a "forum for a true diversity of political discourse." 47 U.S.C. 230(a)(3). The limited protections provided by the statute should be construed with these purposes in mind.

In particular, subparagraph (c)(2) expressly addresses protections from "civil liability" and specifies that an interactive computer service provider may not be made liable "on account of" its decision in "good faith" to restrict access to content that it considers to be "obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable." It is the policy of the United States to ensure that, to the maximum extent permissible under the law, this provision is not distorted to provide liability protection for online platforms that — far from acting in "good faith" to remove objectionable content — instead engage in deceptive or pretextual actions (often contrary to their stated terms of service) to stifle viewpoints with which they disagree.

Section 230 was not intended to allow a handful of companies to grow into titans controlling vital avenues for our national discourse under the guise of promoting open forums for debate, and then to provide those behemoths blanket immunity when they use their power to censor content and silence viewpoints that they dislike. When an interactive computer service provider removes or restricts access to content and its actions do not meet the criteria of subparagraph (c)(2)(A), it is engaged in editorial conduct. It is the policy of the United States that such a provider should properly lose the limited liability shield of subparagraph (c)(2)(A) and be exposed to liability like any traditional editor and publisher that is not an online provider.

(b) To advance the policy described in subsection (a) of this section, all executive departments and agencies should ensure that their application of section 230(c) properly reflects the narrow purpose of the section and take all appropriate actions in this regard. In addition, within 60 days of the date of this order, the Secretary of Commerce (Secretary), in consultation with the Attorney General, and acting through the National Telecommunications and Information Administration (NTIA), shall file a petition for rulemaking with the Federal Communications Commission (FCC) requesting that the FCC expeditiously propose regulations to clarify:

(i) the interaction between subparagraphs (c)(1) and (c)(2) of section 230, in particular to clarify and determine the circumstances under which a provider of an interactive computer service that restricts access to content in a manner not specifically protected by subparagraph (c)(2)(A) may also not be able to claim protection under subparagraph (c)(1), which merely states that a provider shall not be treated as a publisher or speaker for making third-party content available and does not address the provider's responsibility for its own editorial decisions;

(ii) the conditions under which an action restricting access to or availability of material is not "taken in good faith" within the meaning of subparagraph (c)(2)(A) of section 230, particularly whether actions can be "taken in good faith" if they are:

(A) deceptive, pretextual, or inconsistent with a provider's terms of service; or

(B) taken after failing to provide adequate notice, reasoned explanation, or a meaningful opportunity to be heard; and

(iii) any other proposed regulations that the NTIA concludes may be appropriate to advance the policy described in subsection (a) of this section.

Sec. 3. Protecting Federal Taxpayer Dollars from Financing Online Platforms That Restrict Free Speech. (a) The head of each executive department and agency (agency) shall review its agency's Federal spending on advertising and marketing paid to online platforms. Such review shall include the amount of money spent, the online platforms that receive Federal dollars, and the statutory authorities available to restrict their receipt of advertising dollars.

(b) Within 30 days of the date of this order, the head of each agency shall report its findings to the Director of the Office of Management and Budget.

(c) The Department of Justice shall review the viewpoint-based speech restrictions imposed by each online platform identified in the report described in subsection (b) of this section and assess whether any online platforms are problematic vehicles for government speech due to viewpoint discrimination, deception to consumers, or other bad practices.

Sec. 4. Federal Review of Unfair or Deceptive Acts or Practices. (a) It is the policy of the United States that large online platforms, such as Twitter and Facebook, as the critical means of promoting the free flow of speech and ideas today, should not restrict protected speech.

The Supreme Court has noted that social media sites, as the modern public square, "can provide perhaps the most powerful mechanisms available to a private citizen to make his or her voice heard." Packingham v. North Carolina, 137 S. Ct. 1730, 1737 (2017). Communication through these channels has become important for meaningful participation in American democracy, including to petition elected leaders.

These sites are providing an important forum to the public for others to engage in free expression and debate. Cf. PruneYard Shopping Center v. Robins, 447 U.S. 74, 85-89 (1980).

(b) In May of 2019, the White House launched a Tech Bias Reporting tool to allow Americans to report incidents of online censorship. In just weeks, the White House received over 16,000 complaints of online platforms censoring or otherwise taking action against users based on their political viewpoints. The White House will submit such complaints received to the Department of Justice and the Federal Trade Commission (FTC).

(c) The FTC shall consider taking action, as appropriate and consistent with applicable law, to prohibit unfair or deceptive acts or practices in or affecting commerce, pursuant to section 45 of title 15, United States Code. Such unfair or deceptive acts or practice may include practices by entities covered by section 230 that restrict speech in ways that do not align with those entities' public representations about those practices.

(d) For large online platforms that are vast arenas for public debate, including the social media platform Twitter, the FTC shall also, consistent with its legal authority, consider whether complaints allege violations of law that implicate the policies set forth in section 4(a) of this order. The FTC shall consider developing a report describing such complaints and making the report publicly available, consistent with applicable law.

Sec. 5. State Review of Unfair or Deceptive Acts or Practices and Anti-Discrimination Laws. (a) The Attorney General shall establish a

working group regarding the potential enforcement of State statutes that prohibit online platforms from engaging in unfair or deceptive acts or practices. The working group shall also develop model legislation for consideration by legislatures in States where existing statutes do not protect Americans from such unfair and deceptive acts and practices. The working group shall invite State Attorneys General for discussion and consultation, as appropriate and consistent with applicable law.

(b) Complaints described in section 4(b) of this order will be shared with the working group, consistent with applicable law. The working group shall also collect publicly available information regarding the following:

(i) increased scrutiny of users based on the other users they choose to follow, or their interactions with other users;

(ii) algorithms to suppress content or users based on indications of political alignment or viewpoint;

(iii) differential policies allowing for otherwise impermissible behavior, when committed by accounts associated with the Chinese Communist Party or other anti-democratic associations or governments;

(iv) reliance on third-party entities, including contractors, media organizations, and individuals, with indicia of bias to review content; and

(v) acts that limit the ability of users with particular viewpoints to earn money on the platform compared with other users similarly situated.

Sec. 6. Legislation. The Attorney General shall develop a proposal for Federal legislation that would be useful to promote the policy objectives of this order.

Sec. 7. Definition. For purposes of this order, the term “online platform” means any website or application that allows users to create and share content or engage in social networking, or any general search engine.

Sec. 8. 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.

Number 7

Oregon FBI Tech Tuesday: Building a Digital Defense by Recognizing Signs of Trouble

Welcome to the Oregon FBI's Tech Tuesday segment. This week: building a digital defense by recognizing signs of trouble.

Indicators, or symptoms, that your computer or devices have been hacked can vary from nothing identifiable to the most obvious, like getting a ransomware message or having your financial accounts drained.

Some of the more blatant indicators include:

- Your password not working. While this may be a temporary issue with an Internet connection or a requested website having technical issues, it could be an instance in which an attacker has hijacked your account and changed the password.

- People receive emails or social media invites from you that you did not send.

- You get a large number of pop-up ads.

- You get fake antivirus messages.

- You have unexplained online activity.

- You have new browser toolbars, applications, or software which you do not recognize or didn't install.

There also are indicators related to how your computer or device is behaving. For example: your device suddenly slows down, you see a marked increase in data usage, your device randomly restarts, or you are experiencing redirected Internet searches.

Attackers will also use subtle ways to avoid detection. You may notice that your security or anti-virus software has somehow been turned off. The security settings on your device may have been changed, your logging or

registry editor may have been disabled, or system settings may have been altered or disabled.

Trying to identify if you have been hacked and what may have been compromised is a difficult task. Even large corporations with significant financial resources dedicated to cybersecurity fall victim. We hear or read about these incidents all the time.

Organizations shouldn't hesitate to hire professional cybersecurity experts, just as you would hire professional video services for an ad campaign or catering services for a fundraising event. Make sure you do your own research to identify a reputable firm.

Strengthening your systems against attacks and making yourself less of a target for would-be cyber attackers is absolutely critical.

As always, if you have been victimized by a cyber fraud, be sure to report it to the FBI's Internet Crime Complaint Center at www.IC3.gov or call your local FBI office.

Number 8

Preparing for Cyberattacks and Technical Problems During the Pandemic: A Guide for Election Officials

BRENNAN CENTER FOR JUSTICE

Over the past year, many state and local election jurisdictions have taken crucial steps to improve election security, such as replacing paperless voting equipment with paper ballots and disconnecting ballot scanners from networked election night reporting systems.

They have also taken steps to enable a recovery from potential cyberattacks or technical failures, such as requiring polling places to keep emergency paper ballots on hand in case of equipment breakdowns.

Now, election officials face the additional challenge of ensuring secure and safe elections in the midst of a pandemic.

Since officials cannot know at this moment whether all of their voters will feel safe voting in person in November, they must prepare for the possibility that a significant portion will opt to vote by mail.

At the same time, they must maintain in-person voting options, which are necessary for many, including some voters with disabilities and those with poor mail service.

Deploying or scaling up new voting options can increase the risk of technical malfunctions, but officials have no choice in the current environment but to meet the challenge.

Voters are already placing increased demands on online registration systems and mail ballot options.

At the same time, the risk of cyberattacks from foreign state and nonstate actors alike remains.

Many government personnel must work and access election infrastructure remotely now; so too must vendor personnel.

These changes to work environments, if not properly managed, could create new targets for those interested in disrupting American elections through cyberattacks.

Effective digital resiliency plans can ensure that operations continue and eligible citizens are able to exercise their right to vote even in the face of cyberattacks or technical malfunctions.

This document seeks to assist officials as they revise their cyber resiliency plans in light of Covid19. We highlight areas that warrant heightened attention, such as the resiliency of websites and online registration tools.

While we recognize that the pandemic raises a variety of new requirements for election administration, we focus here on resiliency against cyberattacks and technical failures.

In addition to assisting election officials with their plans, this document and the accompanying checklist can help advocates and policymakers working to ensure that election offices are prepared to handle these uncertainties.

Making the changes necessary to run credible and secure elections this November will cost money, and we urge Congress to provide states with the resources they need to ensure that local election officials can run safe and secure elections this fall.

Election Administration and Infrastructure

Due to concerns about Covid-19, election administration is now more than ever being performed and infrastructure accessed remotely.

Election administration and related government functions, such as those carried out by motor vehicles departments, are being undertaken with many employees, including vendors' staff, working from home in order to comply with social distancing guidance and shelter-in-place orders.

Voters and third-party organizations, also subject to these orders and guidance, are similarly using online capabilities to register, renew driver's licenses (thereby having the opportunity to register to vote or update registrations), update addresses, request mail ballots, and look up information, whether about elections and election changes generally or about their status as voters.

Even if states and localities slowly relax shelter-in-place orders, many voters will continue to limit their in-person interactions and will prefer to use online tools for election related transactions.

Personnel, too, may continue working from home.

In any case, the possibility of a local outbreak or overall surge in Covid-19 cases will remain a risk through November.

Any such outbreak may result in renewed shelter-in-place orders and more restrictive social distancing guidance from public health officials.

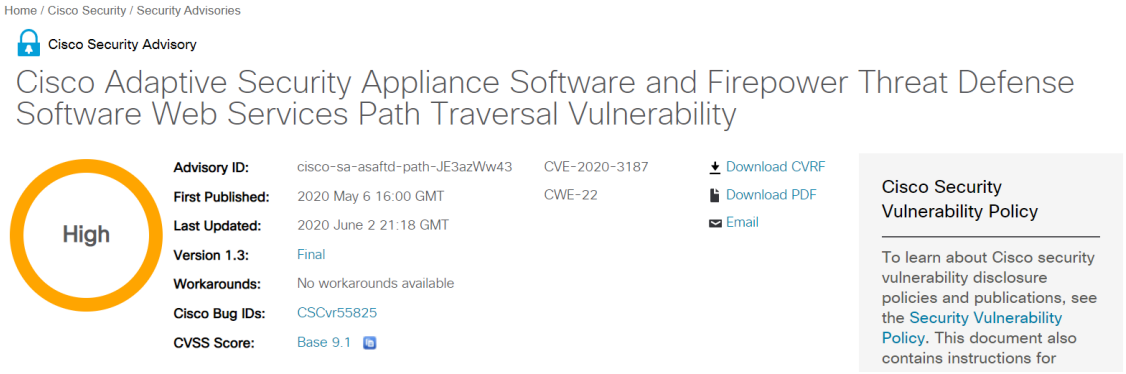
The report:
https://www.brennancenter.org/sites/default/files/2020-06/Resiliency_Final_0.pdf

Number 9

Multiple Vulnerabilities identified by Cisco in their ASA and FTD software and routers

National Cyber Security Centre

Cisco have this week updated an advisory regarding vulnerabilities with their Adaptive Security Appliance (ASA) Software and Firepower Threat Defence (FTD) Software. You may visit: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-path-JE3azWw43


Home / Cisco Security / Security Advisories

Cisco Security Advisory

Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web Services Path Traversal Vulnerability

High

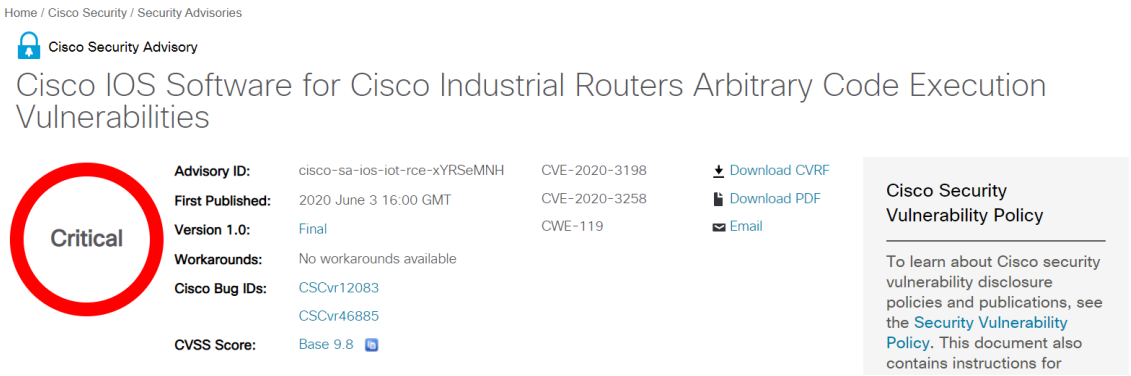
Advisory ID:	cisco-sa-asaftd-path-JE3azWw43	CVE-2020-3187	Download CVRF
First Published:	2020 May 6 16:00 GMT	CWE-22	Download PDF
Last Updated:	2020 June 2 21:18 GMT		Email
Version 1.3:	Final		
Workarounds:	No workarounds available		
Cisco Bug IDs:	CSCvr55825		
CVSS Score:	Base 9.1		

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for

The vulnerability could potentially allow an unauthenticated, remote attacker to conduct directory traversal attacks and obtain read and delete access to sensitive files on a targeted system.

In addition, Cisco have also found multiple vulnerabilities in their IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers and 1000 Series Connected Grid Routers. You may visit: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-iot-rce-xYRSeMNH


Home / Cisco Security / Security Advisories

Cisco Security Advisory

Cisco IOS Software for Cisco Industrial Routers Arbitrary Code Execution Vulnerabilities

Critical

Advisory ID:	cisco-sa-ios-iot-rce-xYRSeMNH	CVE-2020-3198	Download CVRF
First Published:	2020 June 3 16:00 GMT	CVE-2020-3258	Download PDF
Version 1.0:	Final	CWE-119	Email
Workarounds:	No workarounds available		
Cisco Bug IDs:	CSCvr12083		
	CSCvr46885		
CVSS Score:	Base 9.8		

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for

This could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload.

In both advisories, Cisco have included the latest software releases that will address these vulnerabilities for software and routers and at present there are no workarounds available.

The NCSC recommends following vendor best practice advice in the mitigation of vulnerabilities. In this case, the most important aspect is to install the latest software version. Guidance has been published about keeping all devices and software up to date. You may visit: https://www.ncsc.gov.uk/collection/mobile-device-guidance/keeping-devices-and-software-up-to-date

Number 10

NIST Seeks Public Input on Use of Positioning, Navigation and Timing Services

Agency plans guidance to strengthen cybersecurity of related tech, in response to White House order.

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

To bolster the resilience of the Global Positioning System (GPS) and the wide scope of technologies and services that rely on precision timing, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) is requesting information from the public about the broad use of positioning, navigation and timing (PNT) services, as well as the cybersecurity risk management approaches used to protect them.

The request, posted in the Federal Register, is part of NIST's response to the Feb. 12, 2020, Executive Order 13905, Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services. You may visit:
https://www.federalregister.gov/documents/2020/05/27/2020-11282/profile-of-responsible-use-of-positioning-navigation-and-timing-services

NATIONAL ARCHIVES
FEDERAL REGISTER
The Daily Journal of the United States Government

The Executive Order:
https://www.federalregister.gov/documents/2020/02/18/2020-03337/strengthening-national-resilience-through-responsible-use-of-positioning-navigation-and-timing

"GPS and PNT are critical and essential components of the U.S. economy," said Department of Commerce Secretary Wilbur Ross. "It is imperative that our GPS and PNT systems be fully secure and able to withstand cyber incursions. Following President Trump's executive order, the government will continue to test the nation's critical GPS and PNT systems, develop pilot programs to enhance their resilience, and incorporate the best technologies, software and services to safeguard the security and vitality of this crucial infrastructure."

The order notes that "the widespread adoption of PNT services means disruption or manipulation of these services could adversely affect U.S. national and economic security. To strengthen national resilience, the

Federal Government must foster the responsible use of PNT services by critical infrastructure owners and operators."

"Location and timing-based services have become part of the lifeblood of our economy," said Under Secretary of Commerce for Standards and Technology and NIST Director Walter G. Copan. "Not only do we depend upon accurately synchronized GPS satellites to guide us in navigation, but we rely on precision timing to coordinate electricity distribution, synchronize global communications networks, and generate reliable weather forecasts. Securing these PNT-based systems against cyberattack is crucially important for our way of life."

This request, aimed primarily at technology vendors and users of PNT services, contains questions designed to elicit a wide-ranging picture of how PNT is used across different sectors of the economy. NIST will use the answers to inform the creation of a profile document intended to improve the resilience of PNT technologies and services. This document will join the growing list of profiles made to help apply the NIST Cybersecurity Framework to particular economic sectors, such as manufacturing, the power grid and the maritime industry.

NIST is accepting responses to the request until July 13, 2020. For more information, including instructions on how to submit responses by mail or electronically, visit the PNT page on the NIST website at: https://www.nist.gov/itl/pnt

Relevant comments will be posted to the page after the response period closes.

NIST plans to release an initial draft of its PNT profile document this summer. The agency also will solicit public comments on this initial draft before publishing a final version on or before Feb. 12, 2021.

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.

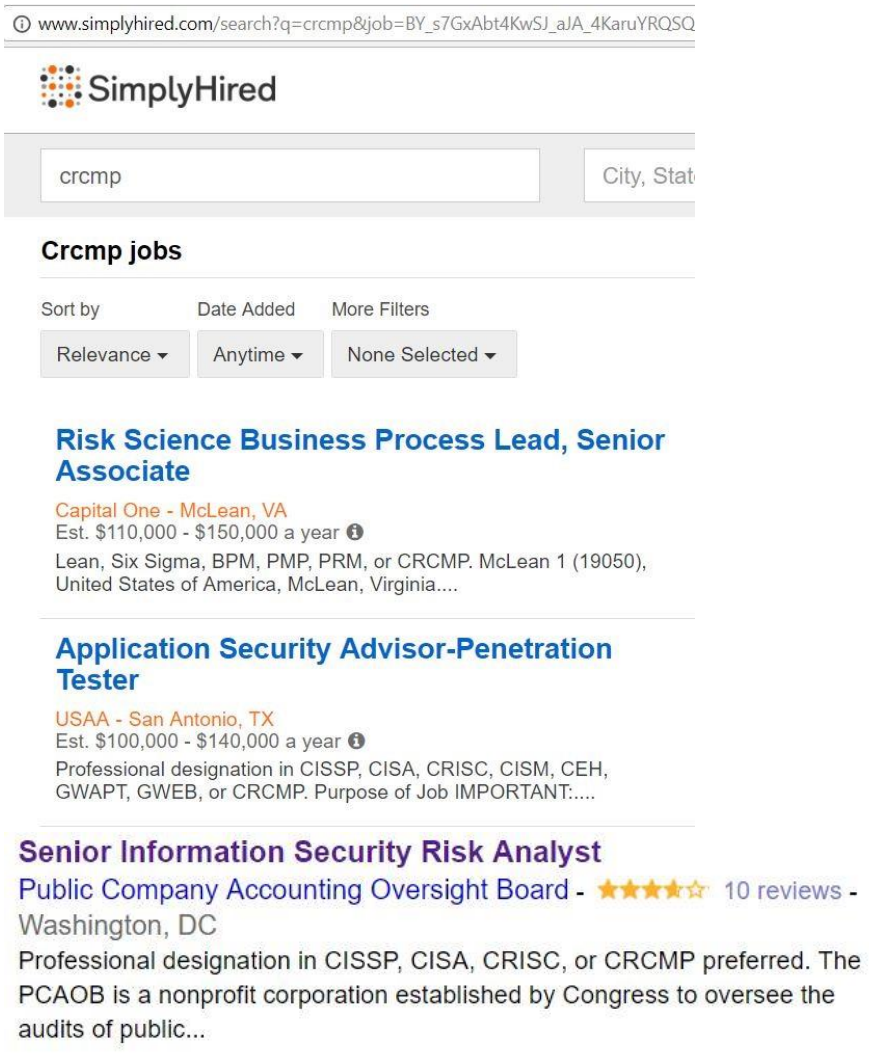
International Association of Risk and Compliance Professionals

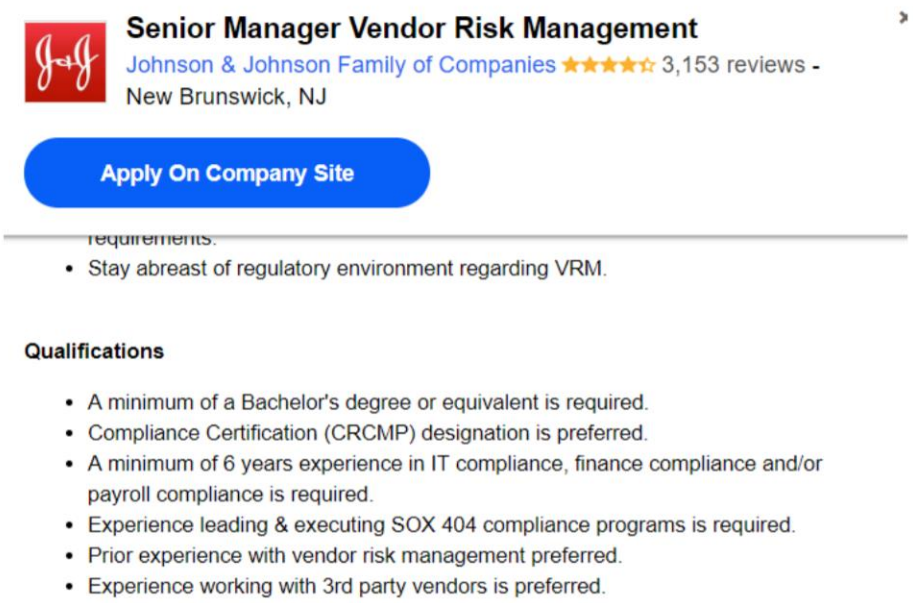
You can explore what we offer to our members:

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