International Association of Risk and Compliance Professionals (IARCP)
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA
Tel: 202-449-9750 Web: www.risk-compliance-association.com

Monday, March 8, 2021

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

Dear members and friends,

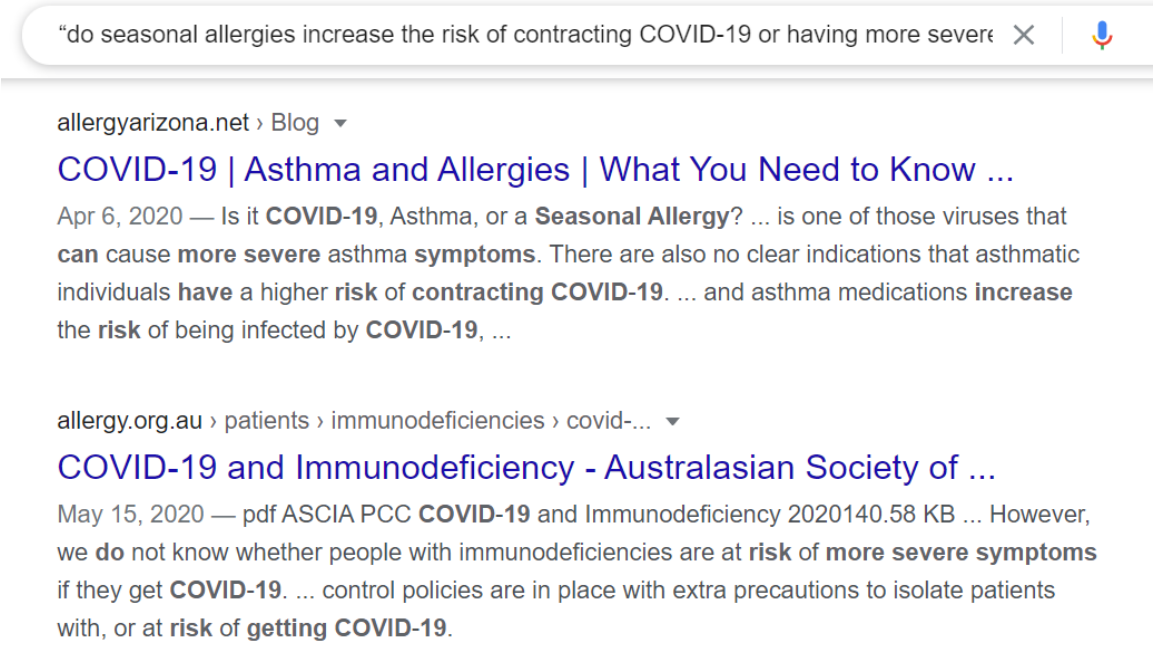
On Monday I had the opportunity to meet an old friend. He told me that he got his website ranked on the first page of Google, and he did nothing for that. I told him that somebody else, perhaps a threat actor, has performed Search Engine Optimization (SEO) techniques to improve the visibility of my friend's website. He laughed and told me I need "some time out to escape paranoid delusion". He also asked me if I often feel threatened and angry, and if I take any antipsychotic drugs.

I could not resist the temptation. On Tuesday I took my second laptop that is used for tests only (Kali Linux on Dell Alienware, never connected to my business environment and to the main router) to investigate what happens with my friend's website. I wanted to investigate if adversaries have used *Search Engine Optimization (SEO) poisoning* to improve the visibility of my friend's *compromised* web site, hoping to infect visitors with malware.

When threat actors compromise a web server, they can replace documents and images with “weaponized” documents and images.

Let us assume that threat actors want to attack a specific group. They may follow the steps:

1. They learn which questions their targets frequently ask online. For example, “do seasonal allergies increase the risk of contracting COVID-19 or having more severe symptoms?”



2. They compromise websites, that are among the first in Google results, when someone asks this or a similar question.

3. They perform Search Engine Optimization (SEO) techniques to improve the visibility of the compromised web sites.

4. They add malicious code and replace documents with identical but infected documents at the compromised web sites. They may try to exploit vulnerabilities in web browsers or to make the visitors download information or images. They may also collect personal information, which can be used in social engineering attacks.

Only imagination is the limit. If I were in their shoes, I would choose “information stealers” like Azorult (that steals the login credentials, cryptocurrency wallets, chat history and credentials, payment card numbers, cookies, and other sensitive browser-based data like autofill information).

For years I have been advised to "avoid visiting unknown websites" and to "always pay attention to the URL in search engine results". Adversaries and state-sponsored groups love checklists and cyber security best practices, as they learn what users usually do. Predictability always introduces vulnerability.

People trust search engines and also trust the results found at the 1st page of the Google results. How in the world could the 1st (out of billions of search results) be dangerous? They click on the first search results without hesitation.

Lucius Annaeus Seneca believed that one of the most beautiful qualities of true friendship is to understand and to be understood. Unfortunately, this was not the case with my old friend. I remembered Antigone by Sophocles: *No one loves the messenger who brings bad news*. Shakespeare (in Henry IV, *and* in Antony and Cleopatra) had the same opinion. They cannot be wrong.

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 6 (Page 26)

The economic outlook- getting back to "more like normal"

John C Williams, President and Chief Executive Officer of the Federal Reserve Bank of New York, at One Hundred Black Men of New York.

Number 7 (Page 31)

EU Electronic Communications Security Authorities Discussion on Incident reports and Policy

Number 8 (Page 34)

BIS Innovation Hub and SWIFT launch ISO 20022 and API hackathon

Number 9 (Page 36)

New NIST Framework Strives for Cleaner, More Secure Power Grid

Number 10 (Page 41)

Technologies to Rapidly Restore the Electrical Grid after Cyberattack Come Online

Number 1

FSB Chair's letter to G20 Finance Ministers and Central Bank Governors

For the past year, the imposition of containment measures across the globe (the "COVID Event") in response to the outbreak of COVID-19 has overshadowed the global economy.

At the outset of the COVID Event, the Financial Stability Board (FSB) focused on emergency measures and actions for what we hoped would be a short-term shock; however, the duration of the Event continues to test our resolve in many ways.

Although the FSB, like many others, faced unprecedented challenges, this year also highlighted certain strengths that the FSB has honed since its inception.

Building on this foundation, three key features of the FSB have characterized members' actions over the past year:

i) responsiveness to crisis;

ii) coordination in action; and

iii) adaptability.

These attributes will certainly help us tackle our most pressing needs going forward, which include addressing vulnerabilities in the global financial system exposed by the COVID Event, as well as ongoing vigilance and monitoring of new and emerging risks.

Through the resilience and adaptability already shown, we will meet our charge of identifying and addressing these risks.

Moving into 2021, the pathway to a post-COVID world is still uncertain. The responsiveness and coordination of the global regulatory community therefore remains as critical now as it was during the past year.

Against this backdrop, the FSB 2021 work program remains ambitious. It seeks to address vulnerabilities directly related to COVID-19 and to increase resilience of non-bank financial intermediation (NBFI).

It also aims to support strong, sustainable, balanced and inclusive growth in a post-COVID world, not least by improving efficiency and access to cross-border payments, and by enhancing our understanding of climate-related financial risks and measures to address these risks, among other key topics.

Addressing COVID-19 Related Vulnerabilities

We have seen some easing of financial market conditions, in part as a result of the significant policy actions taken by G20 members last year; however, challenges to financial stability persist.

The continual assessment of vulnerabilities in the global financial system, therefore, remains a priority and provides a robust basis for cataloging and assessing the impact of COVID-19 policy responses.

Our work to support international coordination on these policy responses includes examining factors needed to prepare for an orderly unwinding of COVID-19 support measures when it is appropriate to do so, including avoiding adverse cross-border spillovers.

Additionally, developing a better understanding of challenges that rising debt levels in the corporate sector may pose is another crucial area of focus. We will report to you on this work in April.

Further, the FSB will provide the G20 an assessment of initial lessons learned from the COVID Event for financial stability, with an interim report in July and a final report in October.

In coordination with other standard setting bodies (SSBs), we will look at financial institutions' use of capital and liquidity buffers and how well crisis management and operational resilience arrangements have functioned.

This work will also examine whether and how procyclicality has affected the financial system.

Any lessons learned at this stage will be preliminary due to the ongoing nature of the COVID Event, but we must begin developing those lessons now, including whether the reforms the G20 put in place following the 2008 Global Financial Crisis are working as intended, and where they may not be.

The FSB will also continue addressing issues identified by the evaluation of too-big-to-fail reforms for banks, the final version of which will be sent to you in April.

Increasing the Resilience of Non-bank Financial Intermediation

One area where we have already begun to draw lessons is NBFI. Our Holistic Review of the Market Turmoil in March 2020 is the basis for a comprehensive and ambitious work program for strengthening the resilience of NBFI.

My November 2020 letter to G20 Leaders highlighted the key areas of this work program, including: examining and addressing specific risk factors that contributed to amplification of the shock; enhancing understanding of systemic risks in NBFI; and investigating policies to address systemic risks in NBFI. This work remains a top priority.

To read more: https://www.fsb.org/wp-content/uploads/P250221.pdf

FSB FINANCIAL STABILITY BOARD

THE CHAIR

24 February 2021

To G20 Finance Ministers and Central Bank Governors

Number 2

Statistical release: BIS residential property price statistics, Q3 2020 - Summary of latest developments

BIS

• Global real house price inflation accelerated to *2.5% year on year (yoy)* in the third quarter of 2020, a period marked by the continued impact of the Covid-19 pandemic and significant fiscal and monetary stimulus.

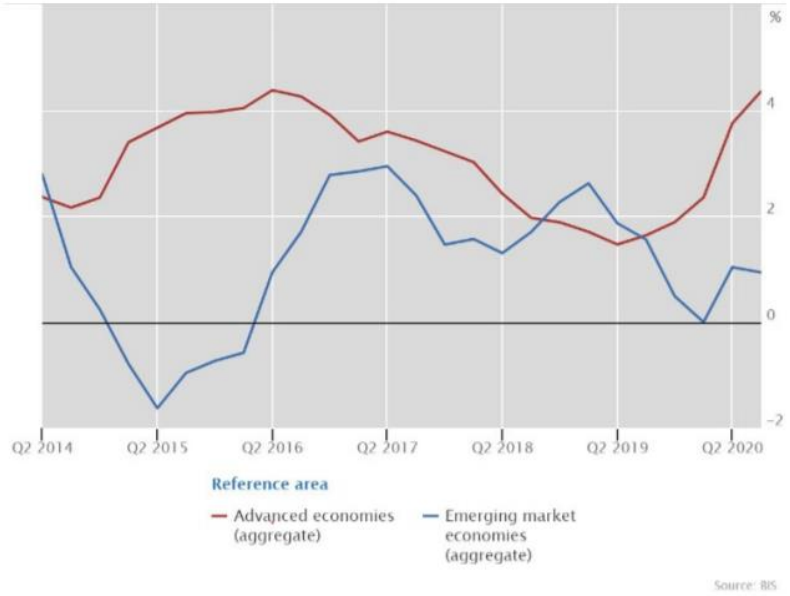
This was primarily due to a significant and relatively widespread expansion in real residential property prices in advanced economies (AEs), by 4.4% on average, the fastest yoy growth rate observed since 2016.

In contrast, real price growth remained subdued (+0.9% yoy) in emerging market economies (EMEs) (Graph 1), with significant differences between central and eastern Europe (+7%), Latin America (+1%), emerging Asia (0%) and the Middle East and Africa (–2%).

• In real terms, global house prices now exceed by 19% the average level recorded immediately after the Great Financial Crisis (GFC) of 2007–09 – and by 23% and 16% for AEs and EMEs, respectively (Table 1).

Aggregate developments in real residential property prices

Year-on-year changes — Graph 1



Source: BIS selected residential property price series based on quarterly average data.

Regional developments in real residential property prices, in per cent, Q3 2020

Table 1

	Cumulative changes since 2010	Year-on-year
All reporting countries	19.3	2.5
Advanced economies	23.4	4.4
Non-European countries	30.5	4.1
Euro area	10.4	5.1
European countries outside the euro area	24.2	3.1
Emerging market economies	16.1	0.9
Latin America	17.2	1.3
Emerging Asia	24.9	–0.4
Central and eastern Europe[1]	–15.6	7.4
Middle East and Africa	9.5	–1.6

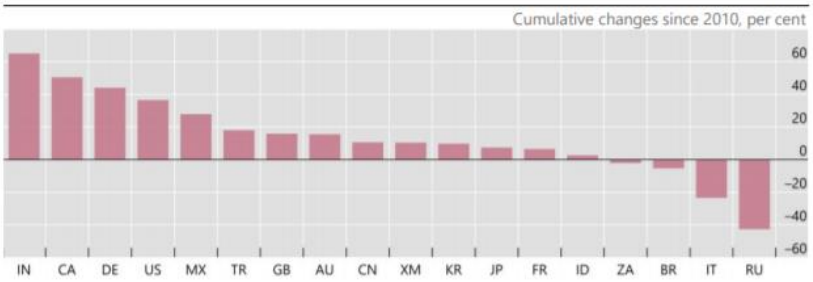
Estimated weighted quarterly averages based on rolling GDP and PPP exchange rates.

[1] Not including members of the euro area.

Source: BIS calculations.

Real residential property price developments in selected countries since the GFC

Graph 2



AU = Australia; BR = Brazil; CA = Canada; CN = China; DE = Germany; FR = France; GB = United Kingdom; ID = Indonesia; IN = India; IT = Italy; JP = Japan; KR = Korea; MX = Mexico; RU = Russia; TR = Turkey; US = United States; XM = euro area; ZA = South Africa.

Source: BIS selected residential property price series based on quarterly average data.

Among G20 economies, real prices have soared over the past decade in India and, though to a lesser extent, in Canada, Germany, Mexico and the United States. At the other end of the scale, they have remained well below their post-GFC levels in Italy and Russia (Graph 2).

To read more: https://www.bis.org/statistics/pp_residential_2102.pdf

Number 3

Atomic Trading

Commissioner Hester M. Peirce, U.S. Securities and Exchange Commission
George Washington University Law School Regulating the Digital Economy Conference

Thank you, Reni [Saula] for that introduction. It is a pleasure to be with all of you today. I will start with the usual disclaimer that my views are my own and not necessarily those of the Securities and Exchange Commission or my fellow Commissioners. The momentous market events of several weeks ago are relevant to the theme of this year's conference—regulating the digital economy—and thus motivate my remarks.

The market events to which I am referring are, of course, the Reddit-threaded run-up in the prices of a number of meme stocks, the subsequent run-down in prices, and the many attendant colorful stories.

At the top of the non-financial news feed were the market volatility, trading volumes, regular Joe-to-riches stories, hedge fund losses, short squeezes, gamma squeezes, glee at sticking it to the "suits," anger at trading limitations, a jumble of emotions as stock prices fell from their highs, and debates about the intricacies of market structure. Movies to elucidate these events are on their way.

The Securities and Exchange Commission, along with other regulators and market watchers, is still sorting through the many layers of those events, so I cannot give you a definitive assessment of what took place, let alone whether any significant regulatory changes or enforcement actions will result.

Instead, I will offer some musings on the challenges that lie before the Commission as we decide whether and how to react to these events with new or modified regulations and, more generally, as we think about stepping up our game as a regulator of the digital economy.

The digital economy enabled the past month's remarkable market events—trading strategies crowdsourced in real time on widely available

social media platforms, instant retail access to the capital markets through handy mobile trading apps, institutional high frequency trading enabled by powerful computing and communications technology responding to and interacting with the retail flows, and sophisticated technology at trading venues and clearinghouses capable of handling record trading volumes. Add some primal emotions into the mix, and the regulator's job in the digital economy can be a difficult one.

Before turning to the challenges of regulating the digital economy, though, I think it is helpful to recognize that, even as our markets undergo technological transformation, our jobs in many ways will remain much as they always have been.

After all, the economy, whether analog or digital, is driven by people; even regulators, at least until the robots replace us, are people. People, with their swirling mix of rationality and emotions are unique, interesting, and complicated.

People are also fallible, frail, and often tempted to abuse power. People respond to incentives. Any effective and fair regulatory framework has to start with a recognition and understanding of people.

A book I read recently about a very different set of market events in a very different time brought the constancy of people's peopleness home to me. These events, like the ones of last month, featured a colorful cast of characters whose fortunes rose and fell and who made their way onto the big screen.

The book tells the story of the uranium markets in the mid-twentieth century, the flames of which were stoked, choked, and revived by the changing policy of the U.S. government's Atomic Energy Commission.

The book's principal author had a bad case of uranium fever, which led him to engage in all sorts of daring adventures to stake uranium claims in the western desert and to raise money to finance them.

He describes to his wife, as she lies in the hospital recovering from an operation, his plan to sell claims to the public in what he explains might be "a real estate deal, a security deal, something similar to an oil lease," or something else.

His wife raises the possibility of jail time, which the author takes as evidence that he "should have known better than to talk business with my wife; she never has the positive-thinking attitude."

His other family members, however, were more positive-thinking; one brother explained:

I've already got blue-chip stock. I've got gilt-edge bonds. I've got my house and car paid for. I've got insurance. If I'd wanted to invest, I know where I could have put my dough. But this was a gamble! I don't want another sure thing. I want to go for the big bundle!

That, the author explained, showed that his family "had the fever. Make it or lose it, but nothing safe, sound, and secure." You may find this hard to believe, but I promise you, I did not pull these lines off Reddit.

A lot of other people had the fever too. The author found them and, through a mailing campaign, got them to send him money:

In mailing, I'd aimed at ordinary Joes, not the professional class, not the ones who were constantly being approached with the deals. I wanted the little people who might never again in their lives have a chance to go for the big bundle for ten dollars down. And the little people liked my deal.

The author reminisces about "the big boom in penny uranium stocks," during which "everyone in the frantic game of trading penny stocks knew that most of them were wallpaper, but that one of them—which one, he didn't know—would be struck by lightning. So buy, buy, buy, and wait for the thunderbolt from the blue."

He further observed that "[w]hen a company admitted that it didn't own its claims and there was absolutely no evidence of uranium, the public rushed to buy stock from such honest people."

The boom went bust when the Atomic Energy Commission pulled its support for further uranium production, which did not trouble the author too much: "There'd be another deal. . . Except for the stockholders. I'd used other people's money."

The book, despite a labyrinth of detours into wholly unrelated topics, contains many other insights into investor psychology, but I think you get the point. People love participating in hot markets, often do so with eyes wide open to the potential for losses and fingers crossed for big gains, and frequently lose real money in the process, and not always money they can afford to lose.

Because the human participants in the digital economy are people, some aspects of regulating the digital economy look a lot like regulating any other kind of economy. One of our regulatory obligations that does not change

much with the times, for example, is—while respecting people's right and capacity to make their own decisions—to remind people of some basic truths about participating in the markets. The medium may change, but the message is the same.

The Commission's Office of Investor Education and Advocacy, for example, issued an investor alert at the end of January to help investors "understand the significant risks of short-term trading based on social media."

The alert contained tips that also would have been helpful for the uranium investors of last century, including a warning about "the rapid rise in the price of an investment, reflecting a high degree of collective enthusiasm or exuberance regarding the investment's prospects [that] is usually followed by a wide-scale selling of the investment that causes a sharp decline in the investment's price" and reminders that you should "[n]ever feel pressured to invest right away" and that you should "not let short-term emotions about investments disrupt your long-term financial objectives."

Although the Commission's delivery method has changed with the times, our investor empowerment message is pretty much the same in the digital world as it was before the digital era. Mr. Taylor's uranium investors would have benefited from such a message as much as today's investors.

So too, our role in policing the markets for fraud has not changed much. As in the past, people often use lies to induce buys, and we bring a lot of enforcement actions to pursue these fraudsters. Although the means of disseminating the lies are digital, the nature of the conduct is not new.

The projects for which funds are being raised may be crypto mining rather than uranium mining, but the fraudsters' plans for the funds raised are generally the same as always—a nice house, fine dining, private school tuition, and maybe some plastic surgery just in case there is a parallel criminal action and a mug shot.

Digital economy regulators are also susceptible to the same incentives and temptations regulators always have faced. Unchanged in the digital world is our obligation to balance our enforcement mission with the need to respect Americans' civil liberties.

We may have new digital tools that make it easier than ever to find bad actors, but they also make it easier to trample over individual rights while doing so. As we put these tools to work for us, we need to bear in mind that when the government watches too much of what a free people do, those people are no longer free.

We have greater and faster insight into trading activity. We can store massive amounts of data. We have computing power and sophisticated software to analyze and work with the data we collect.

Technology enables us to examine individual registered entities remotely, rather than through in-person visits. Structured data allows us to analyze particular registrants or look for trends or patterns across many registrants with the click of a button.

We have access to effective blockchain analytics. And, we have people expert in the use of these tools and the data they generate. One day we may even have easily machine-readable rulebooks, which will foster compliance by regulated entities.

Our regulatory mission will remain the same even as technological developments bring new ways for the capital markets to achieve their core objectives: capital formation and investor enrichment.

To translate that into something more tangible, the goal of our markets is facilitating the flow of investors' money to real companies so they can serve other people's needs and then return money to investors so they can build wealth for themselves and their families.

Technology has the potential to turbocharge the capital markets' ability to achieve this objective. Technological turbocharging is not about speeding up this virtuous cycle. Technology that facilitates unpredictable volatility can undermine the markets' ability to serve investors and companies.

After all, building companies into societally beneficial ventures and building investment nest eggs are slow processes that demand patience, deliberation, and self-discipline. Rather, technology can help markets to deploy capital well, in part by encouraging more of the population to benefit both from contributing capital and using capital to build companies.

But technology does not change our regulatory objectives of protecting investors, facilitating capital formation, and fostering market integrity.

For technology to have its maximum benefit, we will need to change our attitude. Specifically, we tend to look at technological innovation in the markets with deep suspicion, and that mindset has to change.

Attempts to create a good experience using an attractive, easy-to-navigate interface run headlong into a dusty set of regulations written with paper, snail mail, and precise legalese in mind.

We have designed these rules to provide us with static records that are easy to examine rather than to provide actual investors with information in a format they can digest. Investors, conditioned by their experiences with companies in all other sectors, expect more, and our rules should not prevent financial institutions from meeting these expectations.

As one commentator explained, regulators ought not to complain when "online broker-dealers provide an attractive user experience" just as other tech firms do.

Embracing, rather than frowning upon, technology is the only way to achieve our objective of ensuring that investors receive, absorb, and take into account the information they need to make wise investment decisions.

Another part of ensuring that we are not hamstringing the ability of technology to make markets work better for more people is remembering that our role is to protect investors and markets, not incumbents.

Incumbents by definition have adapted themselves well to the existing regulatory framework, market infrastructure, and established technological tools.

They may be slower to adopt new technology; indeed, it may not be in their interest to do so. Resisting regulatory changes that would permit new ways of doing business (or insisting on regulatory changes to forestall technological innovation) may be a matter of life or death for some of these legacy firms.

We regulators should refuse to allow ourselves to be used to block new firms from coming into the industry with fresh, new ways of doing things. We must do what is best for investors and markets.

Decentralized finance will provide a very good test for our ability to regulate with an eye toward protecting the interests of investors and markets, not incumbents.

The anti-Wall Street sentiments coursing through the market events of recent weeks and the growing realization of the power that private and public centralized entities wield in our lives have inspired some to call for throwing the legacy financial system out entirely. In its place, they would put decentralized finance ("DeFi").

The nascent DeFi industry—a rapidly growing corner of the crypto world with significant money involved—is working on building an alternative to the legacy centralized financial system ("CeFi") run through smart

contracts rather than financial intermediaries. DeFi facilitates lending, trading, and investing in crypto-assets. DeFi users trust in smart contracts rather than counterparties.

Although a work in progress with all the growing pains and rough edges that implies, DeFi's promises of democratization, open access, transparency, predictability, and systemic resilience are alluring.

The Federal Reserve Bank of St. Louis recently published a primer on the complicated, multi-layered, fascinating DeFi landscape, which warns of risks including security vulnerabilities, scaling problems, and faux decentralization, but concludes that there is promise in the innovation happening in DeFi.

We regulators, mindful of the potential upsides and downsides, need to provide both legal clarity and the freedom to experiment so that DeFi can compete with CeFi to offer investors financial services.

So what do all of these principles for regulators in the digital era mean for how we will respond to the events of the last several weeks? Some of the sentiment driving the meme stock events seemed to have been rooted in a suspicion that the markets are not for everyone, but that their purpose is to serve only wealthy individuals and institutions.

Some participants seem to have viewed these price rallies and attendant short and gamma squeezes as a way to serve Wall Street a poisonous meal of its own making.

Popular antipathy toward Wall Street fueled by bailouts in the financial crisis of 2007-2009 is still raw, aggravated by ongoing government policies that are viewed as disproportionately benefiting large asset holders now in exchange for an inflationary tab in the future that will hit working Americans hardest.

As securities regulators, we cannot address those concerns directly, but we do need to look for ways to ensure that the markets are working for everyone. Technology is already being used to draw new investors into the markets and to bring capital to companies and entrepreneurs for whom capital raising has until now been difficult.

Increased participation in our markets is beneficial for the markets themselves because, as one commentator explained, "[i]t creates a number of atomized agents providing hopefully unique stimuli and insights to create a more effective and efficient market."

We need to be open to technological improvements that make the markets work better and encourage and equip more people to participate in them. Some commentators have criticized broker-dealers for making investing too easy, or even worse, too much fun, and fun does not necessarily sit well with securities regulators either.

Of course, an appealing user interface is no substitute for ensuring that investors have access to the information that they need to invest wisely in light of their objectives and circumstances, but the same technology that makes investing fun can be used to educate and inform. Indeed, as one commentary on the GameStop events suggested, regulators should be using these same technologies to reach and teach retail investors.

We also could be more proactive in embracing technology to address some of the other concerns that the events of the past month brought to light. While the market machinery worked extremely well under the weight of record trading and high volatility even in the work-from-home COVID world, additional integration of technology into all aspects of the post-trade process might make the system work even better.

Although trading in the digital economy is fast, the process for settling trades is not. Indeed, until 2017, settlement did not occur until three days after the trade date, known as T+3. A regulatory change brought the settlement cycle down to T+2.

As many have been discussing in recent days, further shortening the cycle to T+1 or T+0 could yield additional benefits, including lower risk associated with open positions and reduced collateral demands.

In last week's Congressional hearing, the CEO of Robinhood went even further and called for real-time settlement.

After all, crypto transactions settle quickly and effectively without a central counterparty.

Smart contracts and distributed ledger technology could make the entire clearing and settlement process in the equity markets faster and more efficient.

While new technology may make real-time settlement possible, before deciding whether it is the right solution, we should fully analyze the costs and benefits.

Real-time settlement would address many of the concerns around central clearing and margin calls that we saw late last month.

Widespread adoption of real-time, or at least near real-time, settlement of transactions in equity securities, however, would require a major overhaul in the way equity markets work and could harm liquidity by raising the cost of making markets.

Certain elements of our financial system as it is currently structured work precisely because of the delay between execution and settlement.

An expected drop in margin requirements might not make up for the inability to net transactions, much less the operational risks—and ensuing costs—of settling transactions on a gross basis and transferring large amounts of cash and securities throughout the day.

In addition, the time built into the settlement cycle now makes error correction easier and allows for human intervention, a feature that a smart contract is designed to eliminate.

These uncertainties suggest that a less ambitious approach, focusing on less immediately exciting technological improvements—such as modernizing the post-trade settlement process, which is still excessively dependent on manual intervention and non-standard practices—may allow us to reduce settlement times and clearing costs in a more incremental, yet still significant, way.

Another use for technology is in improving transparency. Many retail investors avail themselves of commission-free trading. Most broker-dealers that offer this benefit to customers offset it with payments from market makers in exchange for the opportunity to interact with retail order flow.

On balance, this practice likely has benefited retail investors, as it has reduced the cost of making a trade and often results in a small improvement of their execution price over the official national best bid or offer.

At the same time, critics are correct when they point out the potential for conflicts of interest on the part of the broker, who may be tempted to send trades to a market-maker who offers worse execution pricing (which hurts the investor) but better payment for order flow (which benefits the broker).

The way to address this potential conflict, though, is not to ban the practice—which would eliminate a potential conflict at the cost of a likely increase in costs to the investor—but to require better disclosure.

As the cost of data processing, presentation, and delivery continues to plummet, our priority should be to leverage technology to ensure that investors receive accurate disclosures about these practices and their effect on execution quality.

Whether we are talking about trading uranium claims for the atomic energy of the past, building communities of atomized retail investors on social media today, or enabling atomic swaps in the DeFi of the future, people's ingenuity and enthusiasm keep us regulators on our toes. In many ways, the regulator's job is unchanged even though the stage is set with more modern scenery.

The digital economy does pose some new regulatory challenges, but it also gives us new tools to meet those challenges. We should use those tools with genuine care for the freedom of the people we regulate. We should welcome the new technology's potential to improve the way markets work and to make them work for more people.

The payoff is high: a successful regulatory framework for the digital economy will unleash its ability to empower individuals to build better futures for themselves, their families, and their communities.

Number 4

ESAs issue recommendations on the application of the Regulation on sustainability-related disclosures

The three European Supervisory Authorities (EBA, EIOPA and ESMA – ESAs) have published a joint supervisory statement on the effective and consistent application and national supervision of the Regulation on sustainability-related disclosures in the financial services sector (SFDR).

The statement aims to achieve an effective and consistent application and national supervision of the SFDR, promoting a level playing field and protecting investors.

In the statement, the three ESAs recommend the draft RTS be used as a reference when applying the provisions of the SFDR in the interim period between the application of SFDR (as of 10 March 2021) and the application of the RTS at a later date.

The ESAs have also set out in an Annex more specific guidance on the application of timelines of some specific provisions of the SFDR, in particular on the application timeline for entity-level principal adverse impact disclosures and for financial products' periodic reporting.

In addition, the Annex includes a summary table of the relevant application dates of the SFDR, the Taxonomy Regulation and the related RTS.

Today's statement complements the recently released Final Report including the draft regulatory technical standards issued by the ESAs Joint Committee on 4 February 2021.

National competent authorities are encouraged to refer financial market participants and financial advisers to the requirements set out in the draft RTS of the final report that has been submitted to the European Commission.

To read more:
https://www.eiopa.europa.eu/sites/default/files/publications/supervisory_statements/jc-2021-06-joint-esas-supervisory-statement-sfdr.pdf

Next steps

The European Commission is required to endorse the RTS within 3 months of their publication. Subject to the non-objection by the European Parliament and Council of the European Union – within 3 months following the Commission's endorsement – the RTS will be adopted by the Commission by means of a delegated regulation.

While financial market participants and financial advisers are required to apply most of the provisions on sustainability-related disclosures laid down in the SFDR from 10 March 2021, the application of the RTS will be delayed to a later date according to the European Commission's letter to the ESAs of 20 October 2020 on the application of the SFDR.

The ESAs have proposed in the draft RTS that the application date of the RTS should be 1 January 2022.

The ESAs will publish in March a consultation paper on taxonomy-related product disclosures under the Taxonomy Regulation which amends the empowerments in Articles 8(4), 9(6) and 11(5) of the SFDR.

esma European Securities and Markets Authority

EBA EUROPEAN BANKING AUTHORITY

eiopa EUROPEAN INSURANCE AND OCCUPATIONAL PENSIONS AUTHORITY

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

JC 2021 06

25 February 2021

Joint ESA Supervisory Statement on the application of the Sustainable Finance Disclosure Regulation

Number 5

BIS Quarterly Review, March 2021, International banking and financial market developments

How much stress could Covid put on corporate credit? Evidence using sectoral data

• This article provides a framework to translate sectoral macroeconomic scenarios into sectoral corporate credit losses, and applies it to the G7 economies, China and Australia.

• Because the pandemic has affected some sectors more severely than others, projected credit losses reflecting sectoral growth paths are very different from those based on projections of aggregate GDP growth alone.

• Despite substantial losses in the sectors most affected by the pandemic, total corporate credit loss rates (ie losses in relation to the stock of debt) could fall short of those during the Great Financial Crisis of 2007–09 because these sectors account for a smaller share of corporate borrowing than at that time.

Introduction

The Covid pandemic triggered the largest economic downturn since the Great Depression. Although the macroeconomic outlook is currently more favourable than it was at the peak of the crisis in the spring of 2020, the second wave of the pandemic is placing an additional strain on the recovery and reinforcing existing vulnerabilities, at least in some of the major advanced economies.

Non-financial corporate (NFC) bankruptcy rates remain fairly low in most countries, despite the sharp decline in economic activity (Banerjee, Cornelli and Zakrajšek (2020), IMF (2020a)).

However, they are expected to rise as measures to support credit are wound back, new consumption habits and business practices accelerate the downsizing of specific sectors, and some firms run out of liquidity buffers (eg Banerjee, Illes, Kharroubi and Serena (2020)).

The looming increase in corporate bankruptcies will generate credit losses that will need to be absorbed, either by the financial system or by taxpayers.

This article assesses potential corporate credit losses at the sectoral level for the G7 countries, China and Australia. On average, corporate credit

accounts for slightly more than half of total private non-financial credit in these countries (ranging from 31% of total credit in Australia to 73% in China) and typically incurs larger credit losses during recessions than household credit.

As such, the outlook for corporate credit has a significant bearing on overall assessments of the health of the financial system.

We project credit losses, defined as recognised impairments on bank and non-bank debt, until the end of 2022, assuming that the pandemic will have played out by then and its impact on credit losses will have materialised.

We proceed in three steps.

First, we construct sectoral economic projections for each of the nine economies in our sample following the approach in Rees (2020).

Specifically, we use a macroeconomic model with a rich industry structure in both demand and production to estimate the economic disturbances ("exogenous shocks") that explain the path of activity since the start of the pandemic.

Conditional on assumptions of how these disturbances play out, we then use the model to project the evolution of sectoral output for each country up to 2023.

In the second step, we combine data on bonds and bank loans to derive corporate debt by sector for each of the G7 countries, China and Australia. The construction of sectoral corporate debt fills a data gap in the public domain.

In the third step, we draw on existing estimates from the literature on the GDP sensitivity of credit loss rates (ie losses in relation to the stock of corporate debt) for banks (Hardy and Schmieder (2013) to translate our sectoral output projections into projected credit loss rates.

In doing so, we assume that the historical sensitivity of bank credit loss rates to aggregate GDP is the same across sectors as well as across bonds and bank loans.

We then scale these sectoral credit loss rates using our estimates of sectoral debt to project total credit losses by sector and country.

We reach three key conclusions.

First, corporate credit loss rates could rise substantially in sectors most affected by the pandemic. The sectoral dispersion in credit loss rates is likely to be wider than during the Great Financial Crisis (GFC) of 2007–09 because of unevenness in sectoral economic conditions as well as the tendency for credit losses to rise more than proportionally with output shortfalls.

Second, aggregate corporate credit loss rates are likely to fall short of those sustained during the GFC, in large part because the sectors most affected by the Covid pandemic account for a comparably small share of total credit.

Third, projected credit losses based on sectoral growth paths are larger than those based on aggregate GDP data alone. This highlights the importance of taking account of sectoral differences in economic conditions and credit exposures when estimating the implications of an uneven recession for corporate credit losses.

To read more: https://www.bis.org/publ/qtrpdf/r_qt2103.pdf

Number 6

The economic outlook- getting back to "more like normal"

John C Williams, President and Chief Executive Officer of the Federal Reserve Bank of New York, at One Hundred Black Men of New York.

Hello, everyone. I'm really pleased to be joining your meeting today. Your work in bringing together leaders and visionaries in support of Black communities across our city is invaluable.

We're approaching the one-year mark since the pandemic took hold. At this time last year there was an increasing sense of fear and uncertainty about the future. And the events since then have posed tremendous challenges to families, communities, and the economy. The ongoing human toll is a tragedy we won't forget in our lifetimes.

What has been an extraordinary public health crisis also has had profound consequences for the American and global economies. The cause of this recession-a global pandemic-means that our economic future will be determined in large part by the path of the virus and our collective success in overcoming it.

We still face many hurdles on the road to recovery from both COVID-19 and the severe economic hardship that has ensued. A lot depends on the success in quickly getting a large part of the public vaccinated against a backdrop of the spread of emerging new strains of the virus.

Despite these challenges and uncertainties, I have become more optimistic about the medium-term outlook for the economy. I don't expect our lives to look like they did a year ago-our sense of "normal" may be forever altered-but with vaccinations well underway and a significant decline nationwide in confirmed new cases, I do expect that we can start to look toward a time that will be "more like normal."

In my remarks today I'll set the scene for the economic picture locally, and for the U.S. economy as a whole. I'll also highlight some of the disparities

we are seeing in the labor market. Finally, I'll share more about the Federal Reserve's response and how I view the path forward.

Before I continue, I need to give the standard Fed disclaimer that the views I express today are mine alone and do not necessarily reflect those of the Federal Open Market Committee (FOMC) or others in the Federal Reserve System.

Dual Mandate

Prior to sharing the outlook, I think it's important to take a step back and explain some of the key factors that my colleagues and I at the Federal Reserve consider in reaching our policy decisions. The Fed has what we call a "dual mandate," which are two goals set by Congress: maximum employment and price stability.

With these goals in mind, our focus is understanding developments that affect labor markets, inflation, and economic growth. But we also collect and analyze enormous amounts of other information, both in the form of data and reports from members of the communities we serve, to help us assess the state of the economy and inform our decision-making.

The Economic Outlook

I'll start off with the most common measure of the overall economy: gross domestic product, or GDP. I expect inflation-adjusted, or real, GDP to rebound sharply this year.

Indeed, with strong federal fiscal support and continued progress on vaccination, GDP growth this year could be the strongest we've seen in decades. Such a robust rebound would be very welcome after the toughest period for the economy in living memory and a winter where the pandemic has been particularly severe.

The resurgence of COVID-19 over the past few months caused consumers to pull back on spending, resulting in significant job losses in some sectors-especially in leisure and hospitality.

In past recessions, we have typically seen a decline in manufacturing jobs, while the service sector-establishments like hotels, bars, and restaurants-was not affected to the same extent. But the pandemic has flipped the script in that regard. Indeed, this time, both the manufacturing and housing sectors have rebounded sharply since last spring, while much of the service sector remains depressed.

The pandemic has had a truly devastating effect on employment. Overall, as of January of this year, we are down nearly 10 million jobs from the pre-pandemic level, a greater shortfall than we saw even at the worst point of the aftermath of the Great Recession.

Locally, we've experienced considerable strain, given that much of New York City's economy hinges on the leisure and hospitality industry. Job losses have been dramatic: New York was hardest hit at the start of the pandemic, and almost a year later the data still show a city under stress. While national employment was 7 percent below pre-pandemic levels at the end of 2020, employment in New York City was 12 percent lower.

I hope that as workers return to their offices and the weather turns warmer we will start to see people frequenting the small businesses that are the lifeblood of our city.

Unfortunately, job losses have not been only highly concentrated in particular industries, but also more concentrated among certain demographic groups. The pandemic and the ensuing economic downturn have done disproportionate harm to women, communities of color, younger workers, and the lowest paid.

The data are particularly sobering when we look at communities of color. Recent research by my colleagues at the New York Fed shows that more Black and Hispanic workers lost jobs compared to white workers, and Black workers have been more likely to drop out of the labor force entirely, making it more challenging to rejoin in the future.

The Black-white unemployment gap, which had reached historical lows in 2019, widened considerably during the spring and summer, undoing much of the progress of the past decade. While the gap has narrowed some since, closing this gap further will be an important part of a full recovery.

Black-owned businesses have also suffered disproportionately. A report released by the New York Fed in August found that Black-owned businesses have been almost twice as likely to shutter during COVID-19 as white-owned firms.

A key area of our focus is to better understand what contributes to economic inequities and to finding solutions.

Through our economic research and outreach efforts, we are working to understand how racial disparities play out in the labor market, and what can be done to change these outcomes.

Now I'll turn to inflation, the other half of our dual mandate. Although we have seen swings in some prices from the effects of COVID, overall the inflation rate has been running below our 2 percent goal.

With our economy and the global economy still far below full strength, I expect underlying inflationary pressures to remain subdued for some time. An encouraging sign is that measures of longer-run inflation expectations have retraced earlier declines as the economic outlook has brightened and are now at levels seen a few years ago.

As the economy fully heals and reaches maximum employment over the next few years, I expect inflation will sustainably move to levels consistent with our 2 percent longer-run goal.

The Path Forward

While the short-term outlook for the economy is highly uncertain, the longer-term picture is more favorable. With the ongoing vaccine rollout, more people will be able to travel, eat out, and shop in person safely.

In addition, the fiscal package enacted in December provides much-needed support to households and businesses until vaccinations are more widespread. Moreover, additional measures are currently being discussed in the Congress. Fiscal support, combined with highly favorable financial conditions and steady progress on vaccinations, are all reasons to be optimistic the economy will experience a strong recovery this year.

But the speed of the recovery will also depend on the global picture. We are seeing a slower rollout of immunizations in parts of Europe and a more subdued rebound in other parts of the world, which will have an effect on the United States. In addition, the emergence of new strains of the virus could slow the path to a post-COVID world.

Our Response

Given all the factors I mentioned earlier, in January the FOMC decided to maintain the target range for the federal funds rate at zero to ¼ percent. The FOMC stated that it expects it will be appropriate to maintain this target range until labor market conditions have reached levels consistent with its assessments of maximum employment and inflation has risen to 2 percent and is on track to moderately exceed 2 percent for some time.

In addition, the Federal Reserve will continue to increase its holdings of Treasury securities by at least $80 billion per month and of agency mortgage-backed securities by at least $40 billion per month until

substantial further progress has been made toward the Committee's maximum employment and price stability goals.

In other words: Despite uncertainties, we are fully committed to supporting the economy through this period and reaching our maximum employment and price stability goals. We will continue to watch and learn and remain committed to using our full range of tools to help assure that the recovery will be as robust as possible.

Conclusion

I'll conclude with this: Despite the progress so far in recovering from the recession, some of the numbers that I've shared are staggering. Families, businesses, and communities are struggling. Almost a year into the pandemic, there is still so much uncertainty.

But despite the near-term challenges, the longer-term outlook for the economy has improved, and our actions of the past year position monetary policy well to support a strong, full recovery and achievement of our goals of maximum employment and price stability. With this progress in mind, I am hopeful for a time soon that looks "more like normal."

Thank you.

Number 7

EU Electronic Communications Security Authorities Discussion on Incident reports and Policy

ENISA hosted the 33rd meeting of European Competent Authorities for Secure Electronic Communications (ECASEC). The group is comprised of EU authorities on security of electronic communications, formerly known as the ENISA Article 13a group.

This 33rd meeting is dedicated to discussions about the incident reports of 2020, the results of the ENISA telecom security legislation assessment of 2020, the draft security profile for the Number-Independent Interpersonal Communication Service (NI-ICS) providers under the European Electronic Communications Code (EECC), the new EU telecom framework.

The group was informed about the ENISA work programme, the Body of European Regulators for Electronic Communications (BEREC) work programme and the European Commission's NIS2 proposal.

The Swiss telecom regulator informed the group about its work on power grid dependencies. The group also selected a Vice-Chair, Ahmet Yesilyurt, a representative of the German authority for telecom security, who will be supporting the Chair, Warna Munzebrock, a representative of the Dutch Radiocommunications Agency.

Details about the meeting

This 33rd meeting was held over 2 days, the first on 18th February and the second, today, the 3rd March. It was attended by 60 experts from national authorities, from EU, EFTA, EEA, and EU candidate countries, who are supervising the European telecom sector.

This is the first of the three regular meetings of the group in 2021. The group will meet again in mid-June 2021.

First day

On the first day of the meeting, the group received an update from BEREC on their present engagements. In the context of forming an opinion for the NIS 2 Directive proposal, BEREC reached the National Regulatory

Authorities (NRAs) through a survey. BEREC presented the results of the survey on the NIS competences of the NRAs.

Boryana Hristova-Ilieva, from the European Commission's DG CONNECT, presented the NIS 2 proposal and answered questions.

Also, ENISA presented the results of the Assessment of the EU Telecom Security Legislation, based on an online survey and interviews of experts working in National Telecom Security authorities and national competent authorities for the NIS Directive.

The outcome of the assessment was overall positive, especially as far as the added value of the ECASEC Group and the role of ENISA are concerned. The need of building trust between authorities and providers was also concluded.

The Group discussed with great interest the upcoming 2021 projects led by ENISA. Getting input from authorities and providers, ENISA is going to analyse sim card swapping attacks and also research consumer outreach strategies on security threats and mitigation measures, which is provisioned in the new EECC.

Second day

Today, the discussions focused on the initial findings steering from the annual incident reports of 2020and the analysis of the 188 incidents reported in 2020. Also the Swiss Regulatory Authority gave an update on their work regarding proposed countermeasures to harden the networks against power problems.

ENISA presented the work on the security profile of the Number-Independent Interpersonal Communication Services (NI-ICS) providers, also known as Over The Top (OTT) providers.

Based on unanimous decision, Warna Munzebrock will continue to be Chair of the ECASEC Expert Group for the next 2 years starting from June 2021 and will be assisted by Ahmet Yesilyurt, a representative of the German authority for telecom security, who is appointed Group Vice-Chair.

Background on ECASEC Expert Group, formerly known as the ENISA Article 13a group

Established in 2010, the ENISA Article 13a Expert Group, now ECASEC EG, consists of more than 50 experts from national telecom security authorities from all EU countries, the EFTA countries, and EU candidate countries.

The group is a forum for exchanging information and good practices on telecom security. It produces policy guidelines for European authorities on the implementation of EU telecom security rules, and publishes annual summary report about major telecom security incidents.

This group has been meeting 3 times per year since 2010, to discuss and agree on a common approach to telecom security supervision in the EU.

This work is done under ENISA's Annual work programme Output O.1.2.3 “Support incident reporting activities in the EU”.

Further Information:
https://www.enisa.europa.eu/topics/incident-reporting

https://resilience.enisa.europa.eu/article-13

Number 8

BIS Innovation Hub and SWIFT launch ISO 20022 and API hackathon

- Hackathon to highlight potential of the new ISO 20022 payments standard and APIs to enhance cross-border payments.

- Teams invited to submit solutions by 19 March.

- Three winning teams will showcase solutions at the BIS Innovation Summit.

The BIS Innovation Hub and SWIFT have launched a new ISO 20022 hackathon and invite teams to build and showcase solutions that enhance cross-border payments, using the ISO 20022 standard for payments messages and application programming interfaces (APIs).

The ISO 20022 Hackathon, which is open for registration until 8 March, aims to highlight the potential of ISO 20022, which is being adopted by large parts of the world's payment infrastructures over the next four years.

Teams can adapt an existing product to make use of ISO 20022 or build and demonstrate new solutions leveraging ISO 20022 and APIs using SWIFT's API sandbox at: https://developer.swift.com/

Three winning teams will showcase their solutions at the BIS Innovation Summit in March to a global audience including key payments industry players and central bankers.

You may visit:
https://web-eur.cvent.com/event/e547cd92-bfcb-4e1e-8dc2-f8f4a2783e2c/summary

To read more: https://iso20022hackathon.hackerearth.com/

Timeline:

- 8 March: deadline for initial proposals;
- 11/12 March: kick-off sessions for successful applicants;
- 19 March: deadline for submission of solutions;
- 23-25 March: winners announced at the BISIH Innovation Summit

Solutions will be judged by a panel including experts from the European Central Bank, Bank of England, Federal Reserve System, SWIFT, Innovate Finance (UK), CPMI, Payments Canada, New Payments Platform (Australia), Swish (Sweden) and DBS Bank (Singapore).

Number 9

New NIST Framework Strives for Cleaner, More Secure Power Grid

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

Whether it's a new set of solar panels glistening on a neighbor's roof or a freshly installed smart thermostat at home, burgeoning renewable and smart technologies represent steps toward a sustainable future. But much of their potential will remain untapped unless the power grid is managed in a much more flexible way.

The ability of systems to speak the same language and exchange information securely, known as interoperability — think syncing your phone to the cloud or your computer — is key to unlocking flexibility on the grid.

Researchers at the National Institute of Standards and Technology (NIST) aim to push interoperability on the grid further than before with the fourth and latest release of the Smart Grid Framework. You may visit: https://www.nist.gov/publications/nist-framework-and-roadmap-smart-grid-interoperability-standards-release-40

NIST Special Publication 1108r4

NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0

The 4.0 version of the framework describes the economic and environmental benefits that could stem from enhanced interoperability and outlines a new strategy for supporting the development of interoperable devices and equipment. The authors also provide guidance and resources for grid cybersecurity, which is becoming increasingly important as greater numbers of devices connect with the grid.

A recent analysis has indicated that, even if all new power generators were zero carbon, continuing to operate the grid as we have for decades will

cause us to fall short of a major goal of the Paris Agreement, which is to limit global temperature rise to 1.5 C (2.7 F).

This finding underscores the need to displace emission sources with renewables. But several hurdles remain that make renewables a challenge for the current system to manage, such as how spread out they are and their fluctuating supply.

“Flexibility is needed to accommodate all of these new clean energy technologies,” said NIST smart grid program manager Avi Gopstein, lead author of the framework.

“The wind doesn’t always blow, the sun doesn’t always shine, and people change the amount of electricity they use depending on their activities. Well, interoperability is all about providing flexibility.”

Interoperable sensors and smart controls could give the grid the flexibility it would need to maintain service during rapid changes in supply and demand.

And part of how they would get the job done is by allowing communication on the grid to become more of a two-way street (between customers and utilities and everything in the middle), making information about current power usage and anticipated need readily available to different parties.

This way, customers would be able to expend resources more intelligently and help utilities route them to the right place at the right time.

An example of interoperability already at play is voluntary rewards programs offered by utility companies, Gopstein said. By using smart thermostats and water heater controllers that are interoperable with their utility’s operations centers, participating consumers are able to contribute to reducing energy consumption during peak demand and receive financial rewards in return.

Homing In on Interoperability Targets

One of the framework’s major offerings is the concept of interoperability profiles, detailed requirements for specific devices that could provide industry with clear targets for interoperability. The ultimate goal of the profiles would be to guide the development of testing and certification programs — a critical ingredient for the widespread use of technology.

“The reason Wi-Fi works on everybody's phone and computer and everything else is because the Wi-Fi Alliance has an effective testing and

certification program," Gopstein said. "They established specific performance requirements and validation tests. For interoperability, we don't have that."

While there are many standard tests for physical performance (for example, a way to check if a 5-volt power supply puts out 5 volts), interoperability is a much more difficult trait to test for.

Hundreds of communication standards exist, meaning there are a multitude of languages devices can speak and myriad ways they can package their messages to other systems.

Rather than develop new standards, Gopstein and his team seek to bring subsets of existing standards for both physical function and communication together in profiles suited to specific types of devices.

If tests are developed based on profiles and widely accepted, manufacturers would have explicit guidance on how to make their devices interoperable with the grid.

These tests could check for proper communication of information such as timing, which, for equipment like smart devices in substations, needs to be synchronized down to the millisecond for conversations between the machines to get off on the right foot.

Over time, as products become certified, the grid would become more of a plug-and-play ecosystem, giving customers more options to choose from.

Protecting the Grid in an Interconnected World

Because the benefits of an interoperable grid would stem from greater connectedness and an increased flow of information between various parties, elements of the grid may become more vulnerable to malicious actors.

The North American Electric Reliability Corporation (NERC) provides a set of mandated security requirements for the high-voltage elements of the grid, such as transmission lines. But for everything else, formal guidance for cybersecurity is scarce, Gopstein said.

The framework offers resources to help fill in these gaps, including a cybersecurity risk profile for the smart grid, which the authors made using NIST's Cybersecurity Framework. The profile, containing numerous security considerations specific to the grid, provides utilities and others with a structured method of assessing their current practices and

identifying areas in need of beefed-up security. The authors also refer organizations to a previous NIST report on smart grid cybersecurity for more detailed guidance at the level of individual device interfaces. You may visit: https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf

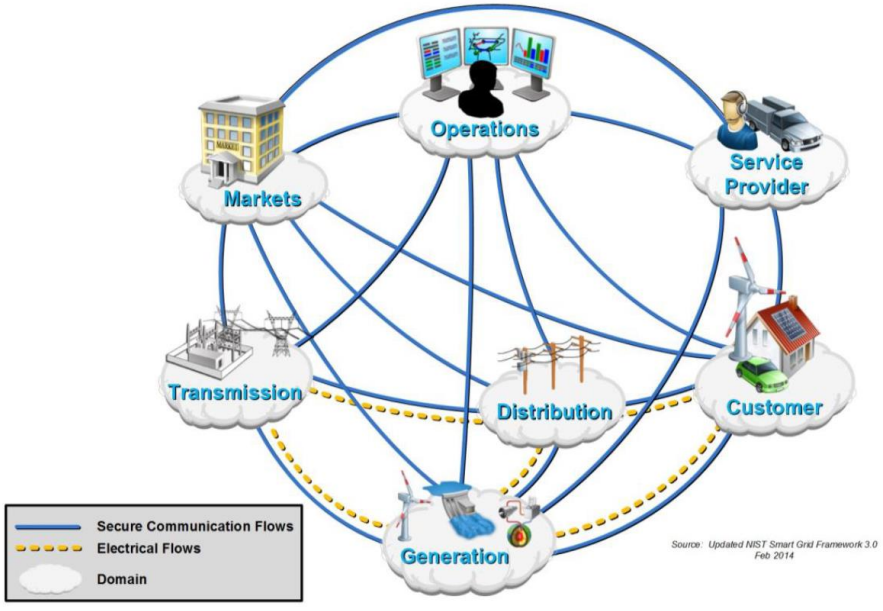
NISTIR 7628 Revision 1

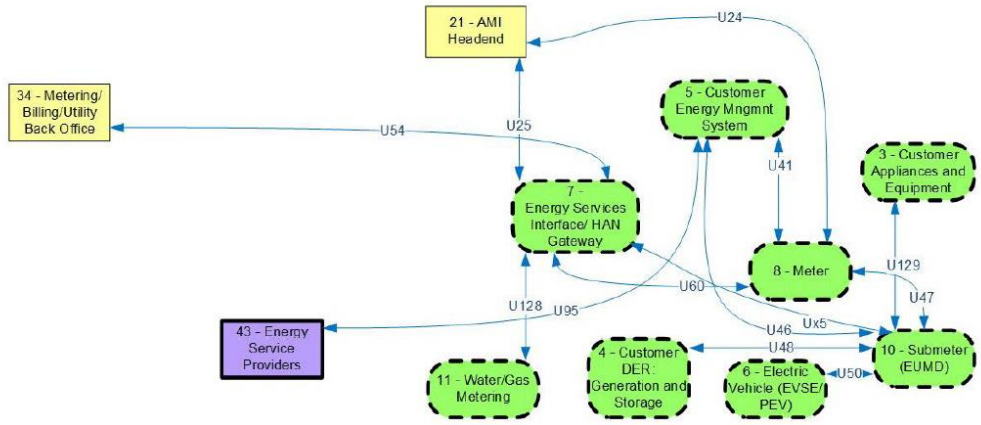
Guidelines for Smart Grid Cybersecurity

Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements

Another important resource the framework recommends is a free tool that highlights overlap between NIST's Cybersecurity Framework and NERC's standards to help organizations improve their cybersecurity practices while ensuring they remain in compliance with mandated requirements.

The fourth release of NIST's Smart Grid Framework, which the authors updated with feedback received through a public comment process, is available for download from NIST's website at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1108r4.pdf




21 - AMI Headend
U24
34 - Metering/ Billing/Utility Back Office
U54
U25
5 - Customer Energy Mngmnt System
U41
3 - Customer Appliances and Equipment
7 - Energy Services Interface/ HAN Gateway
8 - Meter
U129
U60
U47
U128
U95
43 - Energy Service Providers
U46
Ux5
U48
4 - Customer DER: Generation and Storage
10 - Submeter (EUMD)
11 - Water/Gas Metering
6 - Electric Vehicle (EVSE/ PEV)
U50

Number 10

Technologies to Rapidly Restore the Electrical Grid after Cyberattack Come Online

RADICS program delivers novel technologies, custom testbed, and evaluation exercises to enable utilities and first responders to quickly restore critical infrastructure amidst a cyberattack.

Some 330 million Americans rely on the nation's critical infrastructure to keep the country humming. Disruptions to electrical grids, communications systems, and supply chains can be catastrophic, yet all of these are vulnerable to cyberattack.

According to the government's 2019 World Wide Threats Hearing, certain adversaries are capable of launching cyberattacks that can disrupt the nation's critical infrastructure – including electrical distribution networks.

In recognition of the disruptions cyberattacks can cause, DARPA in 2016 established the Rapid Attack Detection, Isolation and Characterization Systems (RADICS) program.

The goal of RADICS has been to enable black-start recovery during a cyberattack.

Black start is the process of restoring power to an electric substation or part of the grid that has experienced a total or partial shutdown without relying on an external power transmission network to get things back online.

Researchers in the program have spent the past four years developing tools and technologies that cybersecurity personnel, utilities, and first responders could use to understand and characterize an attack, isolate networks during remediation, and ultimately accelerate the restoration of power to the part of the grid that has been affected.

The idea is that, if the U.S. can handle the worst case scenario, it will be well positioned to handle other attacks.

"Cyberattacks on the grid can essentially do two things – make the grid not tell you the truth, and make the grid operate in an unexpected way," said Walter Weiss, the program manager responsible for RADICS.

"For example, the grid could show you that a substation has power when in reality it does not. This could unintentionally prevent power restoration to an entire area since no one thinks there is a need to bring power back

online. The technologies developed under RADICS help provide ground truth around grid status, giving responders the ability to quickly detect anomalies and then chart a path towards recovery."

Delivering a Greater Grid

RADICS researchers developed technologies that deliver enhanced situational awareness to grid operators by providing accurate and timely information about grid state before, during, and after an attack. With this improved awareness, operators are better able to thwart an attack or blunt its effects before it can cause significant damage to any physical infrastructure.

To prevent an adversary from continuing attacks on a compromised network during recovery efforts, researchers also developed technologies that isolate emergency networks, allowing for secure responder coordination and communication.

In addition to improving situational awareness, RADICS researchers have developed countermeasures to cyberattacks designed to corrupt configuration files, introduce malicious code in control systems, or perpetrate others types of damage.

Among these countermeasures are tools that could automatically map and assess the state and configuration of electrical power networks and detect and characterize power-grid malware.

To test and evaluate new grid-saving tools developed by RADICS researchers, the program featured a custom-built testbed that replicates real-world conditions that utilities and first responders could encounter during a cyberattack.

To design the testbed, RADICS leveraged over a decade of testbed-architecture work by researchers (and program performers) based at the University of Illinois Urbana-Champaign (UIUC).

The RADICS testbed is comprised of miniaturized substations that were designed to operate as they do in the real world, but with safeguards to protect the system and those operating the substations.

The substations are connected via power lines, forming a multi-utility crank path. With a crank path, power is generated to black start one utility that then powers the next utility and the next until the grid is fully restored. The testbed was designed around commonly deployed systems in North America and configured in ways that actual utilities use.

Further, the UIUC team implemented a distributed, state-of-the-art computer network that allowed for the necessary data collection, dynamic reconfiguration, and adaptation of the environment, which was needed to meet the requirements that Weiss and his team at DARPA specified for the program.

“Testbeds are more than just hardware and software; they are the people, the knowledge, the data, and the assets that are necessary to build out an environment to serve the designed purpose,” said Tim Yardley, the principal investigator responsible for the testbed effort at UIUC.

“The RADICS testbed provided a state-of-the-art environment to explore the unknown, test theories and approaches, and accomplish what has never been tried before – live-fire cyberattacks on critical infrastructure systems in a controlled and observable way.”

Working collaboratively with the Department of Homeland Security (DHS), the RADICS team developed and deployed the testbed at Orient Point, New York, which is home to the DHS Plum Island Animal Disease Center (PIADC).

The island provided an isolated environment for the safe construction and use of the multi-utility crank path.

While first constructed in 2017, the test system was deployed iteratively every six months thereafter to continuously challenge and evaluate the RADICS technology as it advanced and evolved.

Starting in 2017, RADICS tools emerging from the research were put to the test against various threat scenarios during a series of evaluation exercises using the testbed.

The goal of each exercise was to use the technologies to help power the crank path and restore power to a “critical asset” on the island.

Each exercise required consistent communication, collaboration, and problem solving between the research teams and other exercise participants.

Volunteers from organizations responsible for the nation’s electrical grid were recruited by the U.S. Department of Energy (DOE) for the exercises.

These utility volunteers partnered with the research teams to restore power and combat a skilled Red Team as it deployed malicious attacks and exploits.

Utilities having the ability to see a cyber-attack in an exercise prior to seeing it in the real-world enhances emergency preparedness and the robustness of U.S. response efforts. As such, bringing in real volunteers from utilities was critical to making the exercises relevant.

“There was significant participation from our energy sector partners over the two year partnership between DOE CESER and DARPA, resulting in a total of 12 private sector entities sending teams of cyber and power professionals to take part in the exercise and assist DARPA in developing and refining tools” says Michael Toecker, Senior Cybersecurity Advisor in DOE’s Office of Cybersecurity, Energy Security, and Emergency Response (CESER).

“The partnership was equally valuable to our energy sector partners, who had the opportunity to observe and respond to simulated attacks in a consequence-free environment not unlike their own electric power environments.”

The volunteers’ expertise and input continuously helped RADICS improve both the technologies in development as well as the exercise.

The RADICS technologies were tested one last time during a live five-day exercise in October 2020 and the program concluded at the end of the year. This was the seventh exercise in the evaluation series and was conducted jointly with other U.S. departments and agencies – including DOE, DHS, and the National Guard.

An already complex task was further complicated by the COVID-19 pandemic, but the team managed to provide a safe work environment through rigorous testing, limited personnel on the island, and the development of a virtual-presence platform that allowed exercise participants to join remotely.

“With COVID, the UIUC team was asked to accomplish another monumental task – to make the testbed environment seamlessly accessible remotely to the participants that were scattered around the country, while still maintaining a high level of engagement,” said Weiss.

The UIUC team delivered an online/remote environment that enabled the successful execution of the final exercise. Today, other government agencies are looking closely at the remote environment for guidance on how to respond to real-world cyberattacks when resources are spread out.

“The RADICS exercise held at PIADC grew and matured significantly over the lifetime of the program,” said Weiss. “It started out as an exercise

operating in the confines of a lab, and evolved into a three-utility testbed with multiple substations and a supporting virtual environment. By the program's conclusion, we weren't just managing one workforce that was trying to build one crank path across the grid, but three separate 'organizations' that had to work together to figure out how to feed power to each other. The testbed and exercise proved beneficial not only for the program, but also for the broader community involved in grid restoration."

Amplifying Value

Another DARPA program – the Leveraging the Analog Domain for Security (LADS) program – also was able to use the RADICS testbed as a means of program evaluation.

LADS is focused on developing low-cost "cyber smoke detectors" to provide real-time situational awareness for the many devices – like power-grid controllers – that support critical infrastructure and military systems, but cannot be monitored using anti-virus or other current endpoint security technologies.

Under LADS, a team (dubbed CASPER) from New-Jersey-based Perspecta Labs, developed a sensor for detecting anomalous software execution on a SCADA (supervisory control and data acquisition) device from a distance.

The sensor uses machine learning to measure side-channel, radio-frequency (RF) emanations of the device and correlate those emanations with the normal software that runs on those devices.

The CASPER team participated in multiple RADICS exercises, both improving and validating its sensor's performance in a realistic testing environment and, by the final exercise, contributing alerts to warn the RADICS teams of potentially malicious activity in power-grid controllers.

"During the first exercise that the team participated in, the LADS sensors were neither hardened to handle a harsh, real-world environment nor tuned to provide the high-confidence indicators needed to support real-time analysis," said Ian Crone, the DARPA program manager leading LADS.

"By the end of the program, however, the team was able to deploy a ruggedized and reliable sensor to meet the mission need. The RADICS exercises provided a unique environment to test both LADS and other technologies that could really improve power grid security and resilience today and in the future."

A key accomplishment of the final RADICS exercise was the transition of control from the researchers to the participants with day jobs in operational settings. Volunteers from utility companies and the National Guard took over the reins and were able to operate the technologies as they would in a real event. “We often find that research is only usable by the developers or researchers, which in my mind means it’s not operationally relevant,” said Weiss.

“What really changed during exercise seven was this shift from our researchers being the people that operated the tools to the operational people taking charge and running the technologies. This program milestone is helping us chart a path for continued tech transition.”

Perhaps the most significant output of the final exercise however was proof that the RADICS tools are capable of catching threats on the grid. These tools have proven they work in the controlled, testbed environment but also already have transition into commercialized platforms.

One example is Perspecta Labs’ SecureSmart solution. SecureSmart is a system for detecting wireless network intrusions, including those involving SCADAs.

The system provides real-time network health, anomaly detection, security analysis, and visualization. Utilities are currently using the platform for enhanced situational awareness and network visibility, enabling faster response times to threats.

In addition to hastening the transition of RADICS-born technologies for commercial use, the testbed design and accompanying exercise format are expected to transition to the DOE.

These value-added outputs of the program will continue to support training and evaluation efforts for utilities and others in the fight against cyberattacks on the nation’s critical infrastructure.

“DOE CESER and our energy sector partners realized several benefits from working with the RADICS program, most especially in utilizing testbed platforms to inform and enhance exercises, training, and workforce development goals in cyber security for energy systems.

We will be examining where RADICS-style cyber-physical testbeds can and should be used to improve DOE’s preparedness and coordination efforts” said Brian Marko, CESER’s Program Manager for Energy Sector Exercises and Cyber Training.

The UIUC team is working to leverage its RADICS work to support future research and looking into how its new know-how applies to workforce development and training.

Through curriculum and training development, hands-on demonstration platforms, future exercises, and integration with fundamental and applied research, the university researchers will continue to develop, adapt, and advance the platforms they have built to aid the U.S. and help close remaining security gaps.

Girding for More Grid Protection

"While we've made significant progress against RADICS' mission of rapid grid restoration, there remains an opportunity to further explore technologies capable of thwarting attacks, such as enhanced forensic analysis on grid devices to better understand the threats," noted Weiss.

Today, first responders lack ways of interfacing with infected devices, understanding what these devices are doing under malicious influence, and ultimately applying a fix.

Forensics – in this case the practice of deliberately extracting and preserving data about an intrusion – is not yet a supported feature of grid devices. This is further complicated due to the difficulty of removing a device from the grid to understand what happened to it after an attack.

To address this challenge, a team led by SRI International is developing a forensics port that provides a physical opening in these devices for local access to a variety of diagnostic information.

With the port, authorized users can perform a variety of incident response actions, such as memory validation and forensic imaging without compromising vendor IP or a utility's proprietary information.

SRI is sharing the design for this port with DOE, vendors, and other community leaders to jumpstart a discussion on what additional tools are needed to properly equip grid response teams.

Also still to address is the current need for utilities and grid operators to fall back to manual procedures to restore the grid during blackouts if SCADA or EMS functionality is lost.

Today, this involves spending weeks manually creating reliability and resiliency models for tens of thousands of grid nodes.

The process typically requires multiple servers and engineers that must rely on incomplete data for grid restoration. To help accelerate this process, researchers from Carnegie Mellon University (CMU) developed a foundational technology for modeling, simulating, and optimizing power flow of the grid.

The prototype software tool, called Simulation with Unified Grid Analyses and Renewables (SUGAR) provides unprecedented speed and robustness for developing real-time grid models – reducing the process to seconds or minutes from several days – and can be done on a standard laptop.

“The continued research happening at SRI and CMU stands to greatly benefit electrical grid restoration efforts,” said Weiss.

The question of how to prevent an attack from happening in the first place, however still remains. There is additional research happening at DARPA that could help address this challenge by rethinking computer security from the ground up.

The Guaranteed Architectures for Physical Security (GAPS) program is looking at more intelligent ways of connecting in-network computers so that these critical assets are not put on computer networks that are directly connected to the Internet.

“With GAPS, we are looking at how to filter what is allowed so that a device on the power grid, for example, could still upload everything it needs to, but if someone came in remotely they wouldn’t be able to compromise its activities or disrupt the flow of critical data,” noted Weiss who is also leading this program.

The second program is SSITH, which stands for System Security Integration Through Hardware and Firmware. SSITH is focused on developing secure processors capable of thwarting common hardware attacks that derive from software vulnerabilities.

The secure hardware architectures and associated design tools in development on the program could ultimately be used across a wide array of systems, including those found within the electrical grid.

Disclaimer

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

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

This information:

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

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

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

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

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

- is in no way constitutive of an interpretative document;

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

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

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

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

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

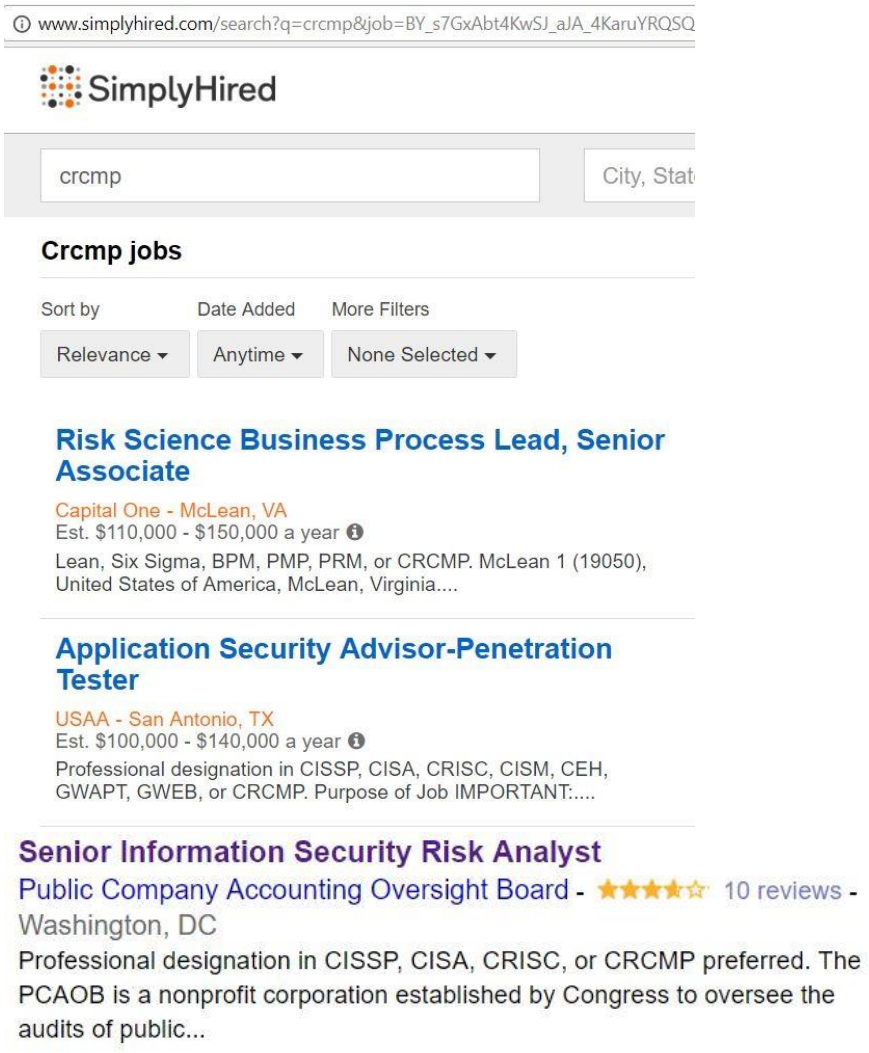
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

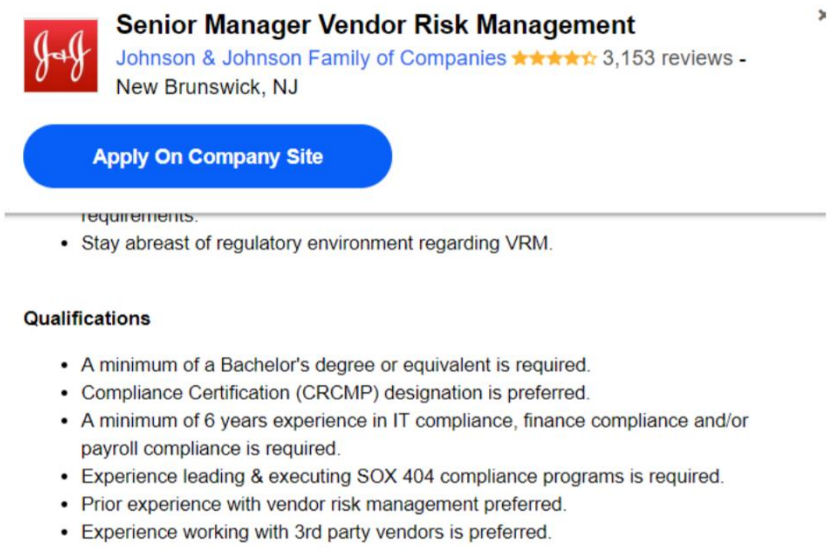
You can explore what we offer to our members:

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

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

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





Senior Manager Vendor Risk Management

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

Apply On Company Site

requirements.

- Stay abreast of regulatory environment regarding VRM.

Qualifications

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

Companies and organizations around the world consider the Certified Risk and Compliance Management Professional (CRCMP) program a preferred certificate. There are CRCMPs in 32 countries. You can find more about the demand for CRCMPs at:
https://www.risk-compliance-association.com/CRCMP_Jobs_Careers.pdf

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

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

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

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

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