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, April 19, 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,

Marcus Tullius Cicero has told: *Live as brave persons; and if fortune is adverse, front its blows with brave hearts.*

Of course, banking regulators do not follow Cicero's advice, but ask for financial stress tests. O tempora, o mores.

I have just read an interesting document that presents the baseline and adverse macro-financial scenarios that banks are required to use in the 2021 EU-wide stress-testing exercise coordinated by the European Banking Authority (EBA).

The aim is to assess the resilience of financial institutions to adverse financial and economic developments, as well as to contribute to the overall assessment of systemic risk in the EU financial system. The adverse scenario sets out paths for key economic and financial variables in a

hypothetical adverse situation triggered by the materialisation of risks to which the EU banking system is exposed.

A stress test is a scenario-based analysis measuring how the banking sector would fare under hypothetical adverse economic developments. The scenario does not attempt to make any predictions about the evolution of the coronavirus (COVID-19) pandemic, but leaves room for a variety of possible negative outcomes (e.g. ineffective vaccine distribution or mutation of the virus). However, the medium-term vulnerabilities arising from the COVID-19 pandemic dominate the scenario.

The COVID-19 pandemic has shaped the EU financial and macroeconomic environment since March 2020. The unprecedented shock inflicted by COVID-19 in 2020, both at the EU level and worldwide, initially led to a sudden halt in economic activity and a sharp deterioration in short term economic prospects.

To mitigate the impact on the economy, governments implemented a number of support measures such as furlough schemes, statutory loan moratoria, government-guaranteed loans, and direct grants. These complemented the monetary policy and prudential actions taken by the ECB and other EU central banks and supervisory authorities.

Nevertheless, the unprecedented slowdown in the economy led to a projected decline in real GDP of 6.9% for the EU in 2020 compared with the figure for the previous year (excluding the United Kingdom), as well as an increase of 0.7 percentage points in the unemployment rate.

As such, the macroeconomic starting point for the 2021 adverse scenario, particularly for GDP, is *significantly worse* than the starting points for the most recent of the previous EBA stress-testing exercises.

Corporate sector indebtedness, already at a high level, paired with the sharp decline in profits, exerts pressure on corporate sector balance sheets. Increasing concerns about the sustainability of corporate debt leads to a widening in corporate credit spreads and a tightening of credit standards, limiting corporates' access to funding for their investments and operations.

The impact on the different sectors is asymmetrical, with the hardest-hit sectors being those that are most severely affected by the containment measures (e.g. travel, air transport, accommodation services, food, and film and media) and those that experience sharp reductions in supply capacity (e.g. sectors engaged in labour-intensive manufacturing, such as textiles and apparel, or those depending strongly on global value chains, such as automotive).

There are some very interesting parts of the stress test. For example, structural changes in commercial real estate demand, exacerbated by COVID-19, trigger a sharp repricing of commercial real estate. The commercial real estate sector faces particularly adverse conditions.

An unparalleled decline in demand for property from certain industries as a result of significant changes in spending habits and business organisation, marked by an increase in remote working and a shift to e-commerce, leads to an abrupt and sustained drop in commercial real estate market activity and strong price corrections over the scenario horizon.

The commercial real estate market experiences substantial repricing, which leads to a cumulative decline of 31.2% at the EU level.

You can read more at:
https://www.eba.europa.eu/risk-analysis-and-data/eu-wide-stress-testing

Welcome to the top 10 list.

*Best regards,*

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

*Number 1 (Page 6)*

## U.S. Economic Outlook and Monetary Policy

Vice Chair Richard H. Clarida, at the 2021 Institute of International Finance Washington Policy Summit, Washington, D.C.

*Number 2 (Page 10)*

## BIS Innovation Summit 2021: How can central banks innovate in the digital age? – watch the videos.

*Number 3 (Page 12)*

## ESAs publish Joint Opinion on jurisdictional scope under the Securitisation Regulation

*Number 4 (Page 14)*

## Technical Guideline on Incident Reporting under the EECC

*Number 5 (Page 17)*

## NIST Offers Tools to Help Defend Against State-Sponsored Hackers

Special Publication 800-172 is designed to protect sensitive information in a variety of electronic systems.

*Number 6 (Page 20)*

## ELECTRICITY GRID CYBERSECURITY

GAO
U.S. GOVERNMENT ACCOUNTABILITY OFFICE

*Number 7 (Page 23)*

## Liquidity to solvency: transition cancelled or postponed?

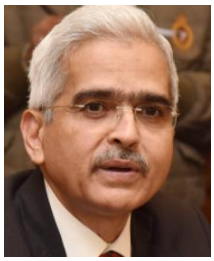
Ryan Banerjee, Joseph Noss and Jose Maria Vidal Pastor

BIS

*Number 8 (Page 25)*

## Financial sector in the new decade

Shaktikanta Das, Governor of the Reserve Bank of India, at the Times Network India Economic Conclave 2021, New Delhi.



*Number 9 (Page 34)*

## EIOPA consults on revised Guidelines on the use of the Legal Entity Identifier

eiopa
European Insurance and Occupational Pensions Authority

*Number 10 (Page 36)*

## Recent Cyber Events: Considerations for Military and National Security Decision Makers

CCDCOE
NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE

*Number 1*

## U.S. Economic Outlook and Monetary Policy

Vice Chair Richard H. Clarida, at the 2021 Institute of International Finance Washington Policy Summit, Washington, D.C.

It is my pleasure to meet virtually with you today at the 2021 Institute of International Finance (IIF) Washington Policy Summit. I regret that we are not doing this session in person, but I do hope next time we will be gathering together in Washington.

I look forward, as always, to a conversation with my good friend and one-time colleague Tim Adams, but first, please allow me to offer a few remarks on the economic outlook, Federal Reserve monetary policy, and our new monetary policy framework.

*Current Economic Situation and Outlook*

In the second quarter of last year, the COVID-19 pandemic and the mitigation efforts put in place to contain it delivered the most severe blow to the U.S. economy since the Great Depression.

Gross domestic product (GDP) collapsed at a roughly 31.5 percent annual rate in the second quarter of 2020, more than 22 million jobs were lost in March and April, and the unemployment rate rose from a 50-year low of 3.5 percent in February to almost 15 percent in April.

Since then, economic activity has rebounded, and it is clear that the economy has proven to be much more resilient than many forecast or feared one year ago. GDP grew by almost 8 percent at an annual rate in the second half of last year, and private forecasters project that GDP will grow roughly 6 percent—and possibly 7 percent—this year.

As shown in the latest Summary of Economic Projections (SEP), the median of Federal Open Market Committee (FOMC) participants' projections for 2021 GDP growth is 6.5 percent.

If these projections are realized, GDP will grow at the fastest four-quarter pace since 1984. And, as this is a virtual meeting of the IIF, I would be

remiss if I did not highlight that if these projections for U.S. economic activity are realized, rising U.S. imports will serve as an important source of external demand to the rest of the world this year and beyond.

As with overall economic activity, conditions in the labor market have recently improved. Employment rose by 379,000 in February, as the leisure and hospitality sector recouped about two-thirds of the jobs that were lost in December and January. Nonetheless, employment is still 9.5 million below its pre-pandemic level for the economy as a whole.

The unemployment rate remains elevated at 6.2 percent in February, and once one factors in the decline in the labor force since the onset of the pandemic and the misclassification of some workers on temporary layoff as employed, the true unemployment rate is closer to 10 percent.

It is worth highlighting that in the baseline projections of the FOMC presented in the latest SEP released last week, my colleagues and I substantially revised up our outlook for the economy, projecting a relatively rapid return to levels of employment and inflation consistent with the Federal Reserve's statutory mandate as compared with the recovery from the Global Financial Crisis. In particular, the median FOMC participant now projects the unemployment rate to reach 4.5 percent at the end of this year and 3.5 percent by the end of 2023.

With regards to inflation, the median inflation projection of FOMC participants is 2.4 percent this year and declines to 2 percent next year before moving back up to 2.1 percent in 2023.

Over the next few months, 12-month measures of inflation are expected to move temporarily above our 2 percent longer-run goal, owing to a run of year-over-year comparisons with depressed service-sector prices recorded in the spring of 2020 and supply bottlenecks limiting how quickly production can respond in the near term.

However, I expect most of this increase to be transitory and for inflation to return to—or perhaps run somewhat above—our 2 percent longer-run goal in 2022 and 2023.

This outcome would be entirely consistent with the new framework we adopted in August 2020 and began to implement at our September 2020 FOMC meeting. In our new framework, we aim for inflation outcomes that keep inflation expectations well anchored at 2 percent.

This means that following periods when inflation has been running below 2 percent—as has been the case for most of the past decade—monetary policy

will aim for inflation to moderately exceed 2 percent for some time. And this brings me to the next topic.

Recent FOMC Decisions and the New Monetary Policy Framework
At our most recent FOMC meetings, the Committee made important changes to our policy statement that upgraded our forward guidance about the future path of the federal funds rate and asset purchases, and that also provided unprecedented information about our policy reaction function.

As announced in the September statement and reiterated in the following statements, with inflation running persistently below 2 percent, our policy will aim to achieve inflation outcomes that keep inflation expectations well anchored at our 2 percent longer-run goal.

We expect to maintain an accommodative stance of monetary policy until these outcomes—as well as our maximum-employment mandate—are achieved. We also expect it will be appropriate to maintain the current target range for the federal funds rate at 0 to 1/4 percent until labor market conditions have reached levels consistent with the Committee's assessments of maximum employment, until inflation has risen to 2 percent, and until inflation is on track to moderately exceed 2 percent for some time.

In addition, in our December FOMC statement, the Committee combined our forward guidance for the federal funds rate with enhanced, outcome-based guidance about our asset purchases.

We indicated that we will continue to increase our holdings of Treasury securities by at least $80 billion per month and our holdings of agency mortgage-backed securities by at least $40 billion per month until substantial further progress has been made toward our maximum-employment and price-stability goals.

The changes to the policy statement that we made over the past few FOMC meetings bring our policy guidance in line with the new framework outlined in the revised Statement on Longer-Run Goals and Monetary Policy Strategy that the Committee approved last August. In our new framework, we acknowledge that policy decisions going forward will be based on the FOMC's estimates of "shortfalls [emphasis added] of employment from its maximum level"—not "deviations."

This language means that going forward, a low unemployment rate, in and of itself, will not be sufficient to trigger a tightening of monetary policy absent any evidence from other indicators that inflation is at risk of moving above mandate-consistent levels. With regard to our price-stability

mandate, while the new statement maintains our definition that the longer-run goal for inflation is 2 percent, it elevates the importance—and the challenge—of keeping inflation expectations well anchored at 2 percent in a world in which an effective-lower-bound constraint is, in downturns, binding on the federal funds rate.

To this end, the new statement conveys the Committee's judgment that, in order to anchor expectations at the 2 percent level consistent with price stability, it will conduct policy to achieve inflation outcomes that keep long-run inflation expectations anchored at our 2 percent longer-run goal.

As Chair Powell indicated in his Jackson Hole remarks, we think of our new framework as an evolution from "flexible inflation targeting" to "flexible average inflation targeting."

While this new framework represents a robust evolution in our monetary policy strategy, this strategy is in service to the dual-mandate goals of monetary policy assigned to the Federal Reserve by the Congress—maximum employment and price stability—that remain unchanged.

*Concluding Remarks*

While our interest rate and balance sheet tools are providing powerful support to the economy and will continue to do so as the recovery progresses, it will take some time for economic activity and employment to return to levels that prevailed at the business cycle peak reached last February. We are committed to using our full range of tools to support the economy until the job is well and truly done to help ensure that the economic recovery will be as robust and rapid as possible.

*Number 2*

## BIS Innovation Summit 2021: How can central banks innovate in the digital age? – watch the videos.

Hear from global leaders on key issues around cross-border and retail payments, central bank digital currencies, banking and the new digital ecosystem, decentralised finance, data, analytics, AI and cloud technologies as well as cultural and organisational changes that may be needed within central banks to meet the challenges of this digital age.


**How can central banks innovate in the digital age?** (00:46:35)
by **Agustín Carstens**, **Gillian Tett**, **Jens Weidmann** and **Jerome H Powell**

**22 Mar 2021** | BIS Innovation Summit 2021


**Cross-border "multi-CBDC" arrangements** (00:07:16)
by **Raphael Auer**

**23 Mar 2021** | BIS Innovation Summit 2021

Cross-border "multi-CBDC" arrangements: what is different from current payment systems, what are the opportunities and what challenges remain?


**Fast, cheaper cross-border payments - is wholesale CBDC the answer?** (00:56:32)
by **Cecilia Skingsley**, **Javier Perez-Tasso**, **Jon Cunliffe**, **Tobias Adrian** and **Umar Farooq**

**23 Mar 2021** | BIS Innovation Summit 2021


**Banking on a new digital ecosystem - new opportunities, business models and regulation** (00:49:20)
by **Douglas Arner**, **Henry Ma**, **Kahina Van Dyke** and **Noah Pepper**

**23 Mar 2021** | BIS Innovation Summit 2021

The videos:
https://www.bis.org/events/bis_innovation_summit_2021/agenda.htm

*Number 3*

## ESAs publish Joint Opinion on jurisdictional scope under the Securitisation Regulation

The European Supervisory Authorities (EBA, EIOPA and ESMA – ESAs) published a Joint Opinion on the jurisdictional scope of the obligations of the non-EU parties to securitisations under the Securitisation Regulation (SECR).

The purpose of the Joint Opinion is to facilitate the understanding of certain SECR provisions in cases where third-country entities become parties to a securitisation.

The Joint Opinion aims to clarify the potential obligations of those third-country parties, as well as related compliance aspects of a transaction under SECR, and is intended to help improve the functioning of EU securitisation markets.

The ESAs, in their Joint Opinion, set out their common view on the practical difficulties faced by market participants in connection with the jurisdictional scope of application of various provisions in the SECR in the following four scenarios:

a) securitisations where some, but not all, of their sell-side parties i.e. originator, original lender, sponsor and special purpose entity issuer etc., are located in a third country;

b) securitisations where all sell-side parties are located in a third country and EU investors invest in them;

c) investments in securitisations by subsidiaries of EU regulated groups, where those subsidiaries are located in a third country; and

d) securitisations where one of the parties is a third country investment fund manager

The Joint Opinion recommends that these difficulties should be addressed, where possible, through interpretative guidance from the European Commission.

The ESAs also invite the European Commission to undertake a comprehensive review of the SECR jurisdictional scope framework as part

of the upcoming overall reform of this Regulation, as a means of thoroughly addressing market participants' concerns regarding proper market functioning.

To read more:
https://www.eiopa.europa.eu/content/esas-draft-opinion-european-commission-jurisdictional-scope-of-application-of_en

*Number 4*

## Technical Guideline on Incident Reporting under the EECC

This document describes the formats and procedures for cross border reporting and annual summary reporting under Article 40 of the EECC. Paragraph 2 of Article 40 describes three types of incident reporting:

1) National incident reporting from providers to CAs,

2) Ad-hoc incident reporting between CAs and ENISA, and

3) Annual summary reporting from CAs to the EC and ENISA.

The focus of this guideline is on the 2nd and 3rd type of reporting: ad-hoc reporting and annual summary reporting.

In December 2018, the new set of telecom rules called the European Electronic Communications Code (abbreviated as EECC) was published and it entered into force.

The EECC updates the EU telecom package of 2009 and paves the way for the roll out of fibre, very high capacity networks and next generation mobile networks (5G). EU countries have to transpose this EU directive into national law by the end of 2020.

An important part of the EECC is consumer protection and security of electronic communications. More services are in scope and the terms security and security incidents are now defined. Article 40 of the EECC contain detailed security requirements for electronic communication providers and article 41 empowers the competent authority with respect to the implementation and enforcement of these requirements.

More specifically, Article 40 requires that providers of public electronic communications networks or services manage security risks posed to the security of networks and services and take security measures including encryption where appropriate. It also requires providers to report about significant incidents to competent national authorities, who should report about these security incidents to ENISA and the European Commission (EC) annually.

This document describes the formats and procedures for cross border reporting and annual summary reporting under Article 40 of the EECC. Paragraph 2 of Article 40 describes three types of incident reporting:

1) National incident reporting from providers to CAs,

2) Ad-hoc incident reporting between CAs and ENISA, and

3) Annual summary reporting from CAs to the EC and ENISA.

The focus of this guideline is on the 2nd and 3rd type of reporting: ad-hoc reporting and annual summary reporting.

Article 40 and 41 of the EECC replace Article 13a and b of the Telecoms Framework directive.

This document replaces the Article 13a incident reporting guideline that was developed by the ECASEC group (formerly the Article 13a Expert Group), under the old legal framework.

The ECASEC Expert Group is a group of competent authorities on telecom security, set up in 2010 to develop a common EU-wide approach to the implementation of Article 13a.

**Figure 1:** Three types of incident reporting in Article 40

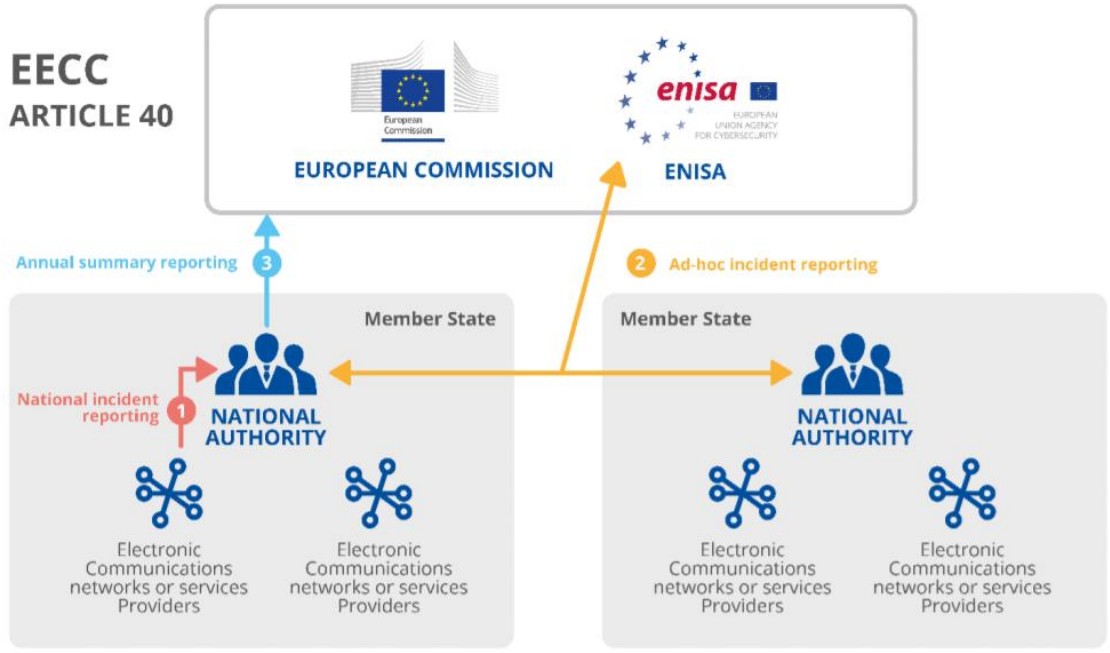
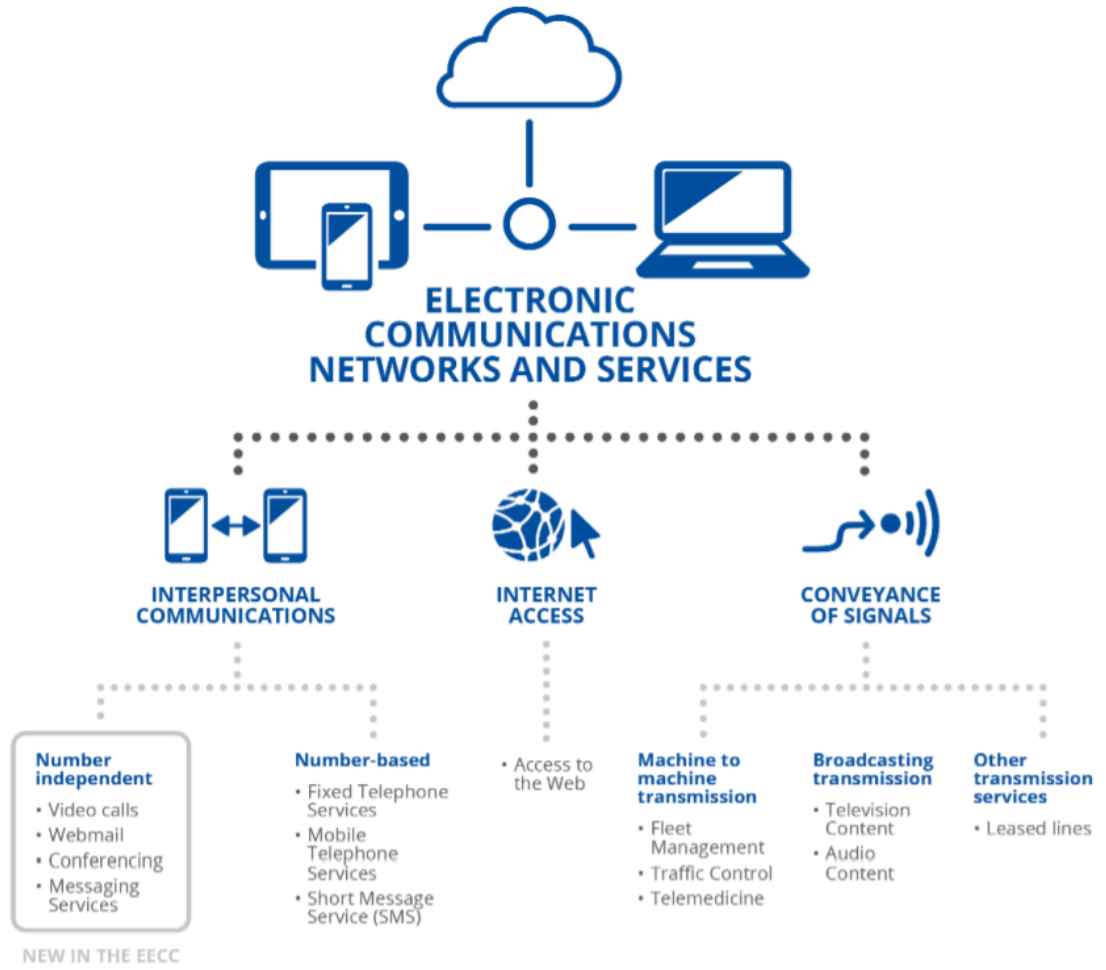


**Figure 2:** Services in scope of EECC




The paper:
https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc

*Number 5*

## NIST Offers Tools to Help Defend Against State-Sponsored Hackers

Special Publication 800-172 is designed to protect sensitive information in a variety of electronic systems.

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

Nations around the world are adding cyberwarfare to their arsenal, employing highly skilled teams to launch attacks against other countries.

These adversaries are also called the "advanced persistent threat," or APT, because they possess the tools and resources to pursue their objectives repeatedly over an extended period, adapting to defenders' efforts to resist them.

Vulnerable data includes the sensitive but unclassified information managed by government, industry and academia in support of various federal programs.

Now, a finalized publication from the National Institute of Standards and Technology (NIST) provides guidance to protect such "controlled unclassified information" (CUI) from the APT. You may visit: https://csrc.nist.gov/publications/detail/sp/800-172/final

NIST's Special Publication (SP) 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST SP 800-171, offers a set of tools designed to counter the efforts of state-sponsored hackers and complements another NIST publication aimed at protecting CUI.

"Cyberattacks are conducted with silent weapons, and in some situations those weapons are undetectable," said Ron Ross, a computer scientist and a NIST fellow. "Because you may not 'feel' the direct effects of the next hack yet, you may think it is coming someday down the road; but in reality, it's happening right now."

The federal government relies heavily on nonfederal service providers to help carry out a wide range of missions using information systems — a term that includes computers, but also a range of other specialized technologies such as industrial control systems and the Internet of Things.

The protection of sensitive federal information that resides in nonfederal systems — such as those used by state and local governments, colleges and

universities, and independent research organizations — is of paramount importance, as it can directly impact the federal government's ability to carry out its operations. A hack in 2018 that compromised sensitive information directly inspired the NIST team's work on SP 800-172.

Formerly numbered SP 800-171B during its draft stages, SP 800-172 offers additional recommendations for handling CUI in situations where that information runs a higher than usual risk of exposure. CUI includes a wide variety of information types, from individuals' names or Social Security numbers to critical defense information.

"We developed SP 800-171 in response to major cyberattacks on U.S. critical infrastructure, and its companion document SP 800-172 is designed to mitigate attacks from advanced cyber threats such as the APT," Ross said.

"Implementing the cyber safeguards in SP 800-172 will help system owners protect what state-level hackers have considered to be particularly high-value targets: sensitive information about people, technologies, innovation and intellectual property, the revelation of which could compromise our economy and national security."

The enhanced security requirements are to be implemented in addition to those in SP 800-171, since that publication is not designed to address the APT. The requirements in SP 800-172 apply to the components of nonfederal systems that process, store or transmit CUI or that provide protection for such components.

To further narrow the scope, the requirements are applied only when the designated CUI is associated with a critical program or high-value asset — the highest priority for protection.

Developed primarily for administrators such as program managers, CIOs and system auditors, the publication addresses the protection of CUI for system components by promoting penetration-resistant architecture, damage-limiting operations, and designs to achieve cyber resiliency and survivability.

Its tools, divided into 14 families, are not intended to be implemented en masse, but selected according to the needs of the organization.

"Most likely an organization implementing this guidance will not want to use all of the enhanced security requirements we offer here," Ross said. "The decision to select a particular set of enhanced security requirements

will be based on your mission and business needs — and then guided and informed by ongoing risk assessments."

In response to feedback received during the public comment period, the final draft includes updated scoping and applicability guidance and a more flexible requirements selection approach to allow organizations to customize their security solutions.

Ross said that the tools in the new publication should offer hope to anyone seeking to defend against hacks, even by as intimidating a threat as the APT.

"The adversaries are bringing their 'A-game' in these cyberattacks 24 hours a day, 7 days a week," he said. "You can start making sure the damage is minimized if you use SP 800-172's cyber safeguards."

You may visit: https://csrc.nist.gov/publications/detail/sp/800-172/final

*Number 6*

# ELECTRICITY GRID CYBERSECURITY

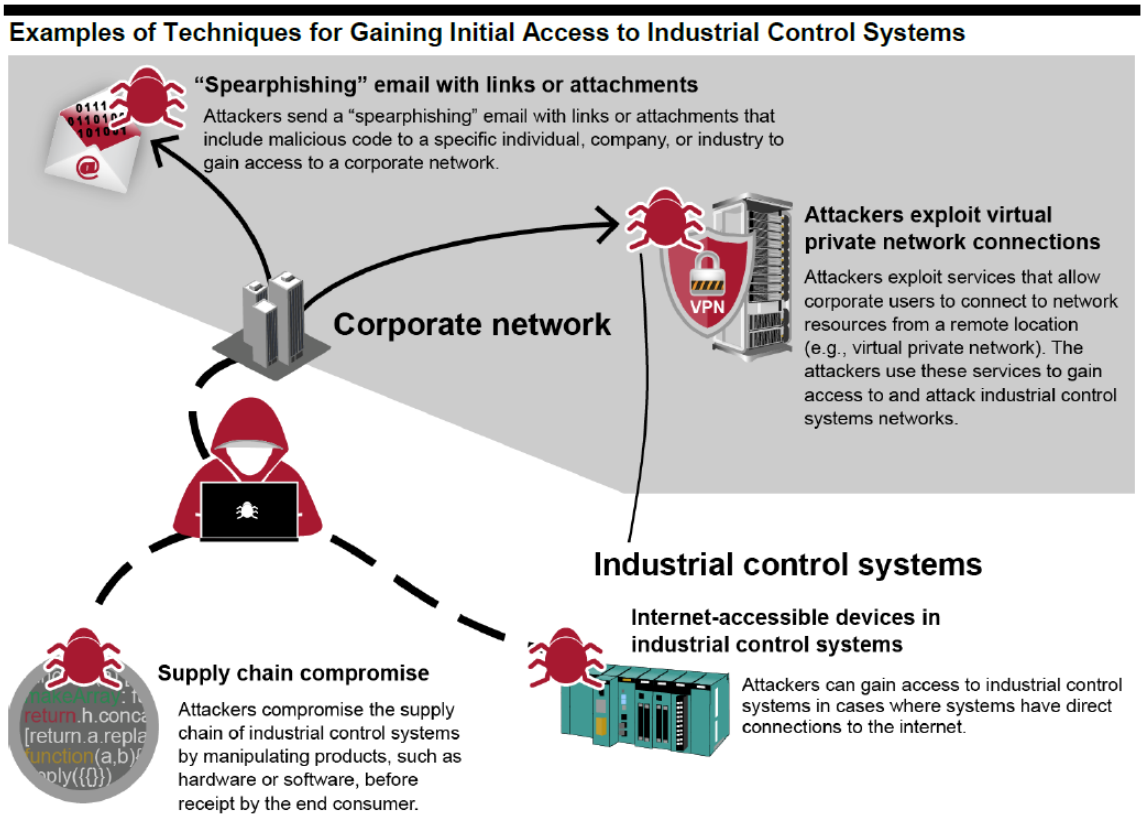
GAO
U.S. GOVERNMENT ACCOUNTABILITY OFFICE

*What GAO Found*

The U.S. grid's distribution systems—which carry electricity from transmission systems to consumers and are regulated primarily by states—are increasingly at risk from cyberattacks.

Distribution systems are growing more vulnerable, in part because their industrial control systems increasingly allow remote access and connect to business networks.

As a result, threat actors can use multiple techniques to access those systems and potentially disrupt operations. (See fig.)
However, the scale of potential impacts from such attacks is not well understood.




Source: GAO analysis of industry and federal documents. | GAO-21-81

Distribution utilities included in GAO's review are generally not subject to mandatory federal cybersecurity standards, but they, and selected states,

had taken actions intended to improve distribution systems' cybersecurity. These actions included incorporating cybersecurity into routine oversight processes and hiring dedicated cybersecurity personnel. Federal agencies have supported these actions by, for example, providing cybersecurity training and guidance.

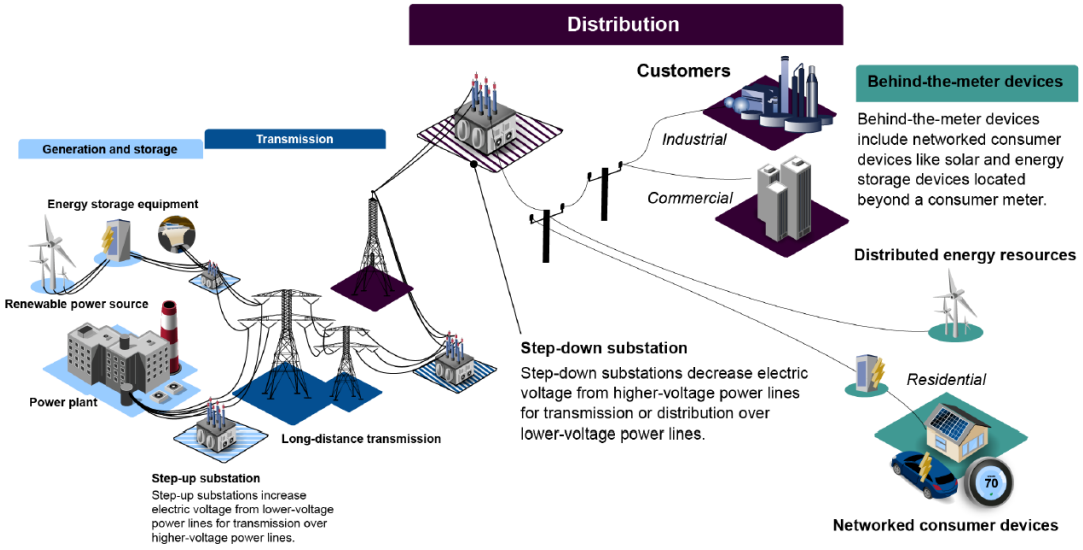
As the lead federal agency for the energy sector, the Department of Energy (DOE) has developed plans to implement the national cybersecurity strategy for the grid, but these plans do not fully address risks to the grid's distribution systems.

For example, DOE's plans do not address distribution systems' vulnerabilities related to supply chains.

According to officials, DOE has not fully addressed such risks in its plans because it has prioritized addressing risks to the grid's generation and transmission systems.

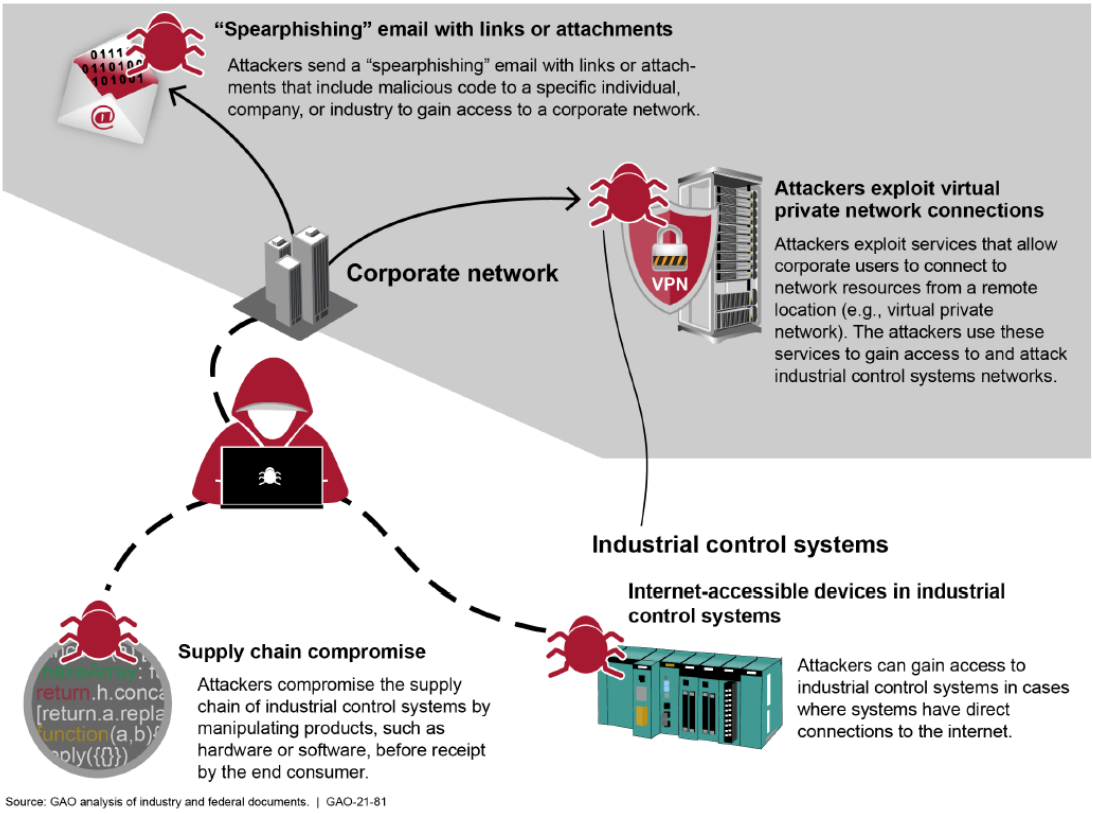
Without doing so, however, DOE's plans will likely be of limited use in prioritizing federal support to states and industry to improve grid distribution systems' cybersecurity.

**Figure 1: Functions of the U.S. Electricity Grid**




Sources: GAO; Art Explosion (images). | GAO-21-81

Figure 2: Examples of Techniques for Gaining Initial Access to Industrial Control Systems




Source: GAO analysis of industry and federal documents. | GAO-21-81

To read more: https://www.gao.gov/assets/gao-21-81.pdf

*Number 7*

## Liquidity to solvency: transition cancelled or postponed?

Ryan Banerjee, Joseph Noss and Jose Maria Vidal Pastor

BIS

*Key takeaways*

• Since the start of the Covid-19 pandemic, a "bankruptcy gap" has emerged between measures of expected and realised bankruptcies globally.

• The ample supply of credit to make up for short-term losses has been an important factor decoupling bankruptcies from the sharp reduction in firms' cash flows.

• Firms' reliance on credit suggests that it may be too early to dismiss future solvency risk.

Significant increases in leverage and weak earnings forecasts in some sectors suggest that for some firms, greater credit extension may have only postponed, rather than cancelled, their insolvency.

Not too long ago it was conventional wisdom that the global economy would transition from the "liquidity phase" to the "solvency phase" of the Covid-19 economic crisis. A large wave of insolvencies was expected.

So far, however, insolvencies have remained very low, and even fell in many jurisdictions during 2020 (Banerjee, Cornelli and Zakrajšek (2020), IMF (2021)). As a result, a gap has opened between previously reliable predictors of bankruptcy rates based on economic activity and actual realised bankruptcies.

We refer to this phenomenon as the "Covid-19 bankruptcy gap". This bulletin aims to shed light on the drivers of this bankruptcy gap and identifies two important determinants.

First, the impact of the pandemic has been highly asymmetric. Although it has hit consumer facing sectors exceptionally hard, other sectors less affected by the pandemic (and its associated containment measures) experienced a strong recovery in Q3 2020.

Moreover, the ability to recoup missed revenues has alleviated insolvency stresses, particularly in the durable goods sector. That said, this falls short of a satisfactory explanation of why bankruptcies have been so low, even falling in some economies.

The second and, arguably, more important factor suppressing bankruptcies has been the ample supply of credit, facilitated by unprecedented monetary and fiscal support.

This has been pivotal in preventing insolvencies, because it is ultimately insufficient cash flows that give rise to bankruptcies (Banerjee and Kharroubi (2020)).

After all, firms go bust when they cannot pay their bills. Ample credit during 2020 stands in sharp contrast to the Great Financial Crisis (GFC) when credit conditions were exceptionally tight.

Whilst the increase in credit has prevented business firms' insolvency in the short term, it has also increased their indebtedness. In an optimistic scenario, with the global vaccine roll-out being successful, business models of the vast majority of firms in the hardest hit sectors will continue to be fundamentally sound and cash flows will recover to pre-Covid-19 levels.

The risk of a significant rise in "zombification" will be low under this scenario. However, firms' indebtedness will be higher, and this might result in changes of firm ownership from equity holders to creditors. Perhaps the more worrying scenario is the combination of higher debt levels and depressed earnings for credit dependent firms in some sectors, as suggested by consensus forecast estimates for 2021.

Under this scenario, firms in the airline, hotels, restaurants and leisure sectors would remain highly dependent on additional support to avoid insolvency. These risks could be compounded if vaccines are less successful in containing the spread of Covid-19. Prolonged weakness in these sectors could in turn spill over into the more leveraged commercial real-estate sector.

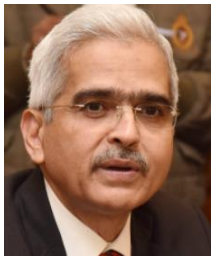
The uncertain outlook for firms' cash flow and the role of credit in containing bankruptcies to date shines a spotlight on banks' loss-absorbing buffers and provisioning strategies, as well as on accommodative financial conditions and government guarantees that have sustained credit to struggling firms.

To read more: https://www.bis.org/publ/bisbull40.pdf

*Number 8*

## Financial sector in the new decade

Shaktikanta Das, Governor of the Reserve Bank of India, at the Times Network India Economic Conclave 2021, New Delhi.



A very warm good morning to you all. It is indeed an honour for me to be here at the India Economic Conclave 2021 organised by the Times Network. I have been looking forward to participating in this year's conclave, especially after an enriching experience during my participation in this event in 2019.

The theme of this year's conclave, one which resonates very strongly is "India's Decade: Reform. Perform. Transform." The COVID-19 pandemic has set forth the wheels of transformation for everything around us, from our work life to our policy priorities. As we toil towards addressing the challenges raised by COVID-19 with the aim to emerge as a modern and transformed India, I applaud the foresight of the Times Network in selecting such a pertinent theme.

2. Today in my address, I have chosen to speak on a subject in which the Reserve Bank has a major stake – "financial sector in a new decade". Contextually, it is important to bear in mind that unlike the global financial crisis (GFC) of 2008 when financial sector vulnerabilities impacted the real sector, this time the risk of contagion is from the real sector to the financial sector.

*Global Perspective*

3. Globally, the measures initiated in the last decade after the global financial crisis were aimed at reducing leverage and improving the quality and quantity of capital, among others. As a result, before entering the Covid pandemic, banks were well capitalised and maintained high liquidity buffers, which - coupled with loan moratorium and asset classification freezes - helped them to stay resilient during these tough times.

Measures taken by central banks and national governments such as reducing policy rates; capital, liquidity and regulatory relaxations; asset purchases; forex swaps; and government guarantees, among others, played

a crucial role in preventing heavy sell-offs and protecting bank balance sheets. This collective endeavour resulted in stabilisation of the financial sector and provided necessary liquidity support to maintain the flow of credit in the economy.

The rapid progress in vaccine has upgraded the global outlook although we are not out of the woods yet as fresh waves of newer variants of the virus bring in fresh concerns. While the global economy continues to reel under the impact of this unprecedented shock, the near-term financial stability risks have been contained on account of coordinated interventions of central banks across the globe.

4. The present pandemic underlines the imperative of strong capital buffers in the banking system. While the capital reforms undertaken post GFC did provide space to cushion the immediate impact of the current pandemic, banks would need to shore up their capital position, both to absorb some of the slippages as well as to sustain credit flow, especially when monetary and fiscal measures unwind.

While part of the global regulatory reform agenda is still under implementation, the pandemic provides an opportunity to test and evaluate the efficacy of various reform measures. The learnings from the crisis could throw up new focus areas to be addressed in the design of the international regulatory architecture for banks and other financial sector entities.

*Indian Context*

5. In the Indian context, maintaining the health of the banking sector remains a policy priority. As I have stressed on several earlier occasions, the strength of a banking system depends on building its capital base while at the same time focusing on corporate governance and ethics-driven compliance culture.

Banks and NBFCs need to enhance their skillset to identify risks early, measure them, mitigate the risk proactively and build up adequate provisioning buffers to absorb potential losses. They should also augment their internal stress testing framework with severe but plausible stress scenarios. Upgradation of IT infrastructure and improving customer services together with cybersecurity measures are other key issues which also need attention.

6. On our part, we have reorganized RBI's supervision of banks, non-banking financial companies (NBFCs) and urban co-operative banks (UCBs) under one umbrella and initiated a series of measures to strengthen supervisory oversight on these entities. Our focus is more on early

identification of risks, putting in place a structured early supervisory intervention framework and increasing the focus on root causes of vulnerabilities than on symptoms. We are also harmonising the supervisory rigour across banks and NBFCs.

7. The Reserve Bank has also been taking steps to provide all round support to improve the resilience of these sectors. Apart from liquidity support through targeted long-term repos (TLTRO) and special liquidity support windows, other measures included priority sector classification benefit to banks' lending to NBFCs for on-lending to priority sector, promoting co-lending model, harmonisation of exposure limits for banks' exposure to NBFCs under the large exposure framework, synchronisation of risk weights for exposures of banks to rated NBFCs with those of corporates, and relaxations for minimum holding period for securitisation and assignment.

We have also strengthened the liquidity risk management framework with the introduction of granular maturity buckets and glide path for introduction of liquidity coverage ratio (LCR) for NBFCs. To augment risk management practices, a functionally independent Chief Risk Officer (CRO) with clearly specified roles and responsibilities was mandated for large NBFCs.

The guidelines for Core Investment Companies (CICs) were revised in August 2020 with a view to address complexity and multiple leveraging, strengthen risk management and corporate governance practices, and induce transparency through disclosures.

The revised regulatory framework for Housing Finance Companies (HFCs), issued in October 2020, aimed at harmonising the regulations between HFCs and NBFCs in a non-disruptive manner. Further, keeping in view the increasing significance of NBFCs in the financial system, we are in the process of finalising the guidelines on their dividend distribution and scale based regulation.

8. The UCBs are registered as cooperative societies and have been under the dual regulation of the Reserve Bank and the Central/State Registrar of Cooperative Societies (RCS). The recent amendments to the Banking Regulation Act, 1949 (as applicable to Cooperative Societies) has brought the functions of governance, capital, audit and amalgamation of co-operative banks under the regulatory domain of the Reserve Bank.

In the recent period, we have been taking measures to improve their governance structure, implement system-based asset classification norms, bring them into the CRILC1 reporting infrastructure and under the

supervisory action framework (SAF). Last month, we have set up an expert committee to examine these issues and provide a road map for strengthening the UCB sector.

*Banking sector: Way Ahead*

9. The Reserve Bank is striving towards a more competitive, efficient and heterogeneous banking structure. The licensing policies for universal banks, small finance banks (SFBs) and payments banks are a step in this direction. Presently, ten SFBs and six payments banks are operational.

10. I foresee four distinct sets of banking landscapes emerging in the current decade.

The first set will be dominated by a few large Indian banks with domestic and international presence.

Second, there will be several mid-sized banks with economy-wide presence.

The third set would encompass smaller private sector banks, SFBs, regional rural banks and co-operative banks, which may specifically cater to the credit requirements of small borrowers.

The fourth segment would consist of digital players who may act as service providers directly to customers or through banks as their agents or associates. In fact, digital players would increasingly emerge as critical pieces across all segments.

11. Let me now dwell upon the interplay and synergies that could be exploited by these four segments while they compete with each other to move up the ladder. Each of these segments needs to comprehend the future needs of the society and respond to the growth in the Indian financial sector. IT systems need to be developed to handle the exponential surge in the number of transactions.

The example of Unified Payments Interface (UPI) which took three years' (2017-2019) to register a monthly count of 1 billion transactions, but doubled to 2 billion a month in a short span of another year clearly stands out. This demonstrates the need for scalability of systems and platforms in such a way that it can be easily scaled up, not 'incremental scalability, but 'exponential scalability'.

12. India is on the way to becoming Asia's top financial technology (FinTech) hub with 87 per cent FinTech adoption rate as against the global average of 64 per cent.

The FinTech market in India was valued at ₹1.9 trillion in 20192 and is expected to reach ₹6.2 trillion by 2025 across diversified fields like digital payments, digital lending, peer to peer (P2P) lending, crowd funding, block chain technology, distributed ledgers technology, big data, RegTech and SupTech, to name a few.

In a world where the FinTech companies are leading in terms of the volume of digital transactions and playing a more active role in the banking and finance industry, it is important that the commercial banks adapt to the technological changes and work in tandem with these entities so that in future they are part of the ecosystem rather than competing with Fintech companies for business. A meaningful collaboration and co-existence in providing affordable and efficient value-added services would help both the worlds.

13. From the regulatory perspective, it is RBI's priority to foster effective regulations with continuous knowledge acquisition so that we stay ahead of the curve. The Reserve Bank's endeavour is to ensure that the regulations do not constrain innovation; rather they should encourage and nurture innovation, without compromising the need for financial sector stability, cybersecurity, customer protection, etc.

Optimality in regulation and supervision is the key. With this objective in mind, we have recently constituted a working group on digital lending, including lending through online platforms and mobile apps. Overall, an orderly growth of Fintechs will benefit all the stakeholders in the financial sector.

*Financial Sector and Payment System – Lifeline of the Economy*

14. While we are on Fintech and technology, it would be extremely relevant to touch upon the developments in our payment systems where India has shown remarkable progress in recent years. As the adage goes "the best way to predict the future is to create it" and at the Reserve Bank, this is our unwavering approach when it comes to the future of payment systems.

With our commitment to foster innovation, and provide state-of-the-art and safe experience to users, we have placed ourselves in the forefront of payment systems on a global stage. India has emerged as one of the leaders when it comes to payment systems; perhaps akin to the recognition in the COVID vaccine front. Sustaining this position is both challenging and exciting.

15. The growth rate of Indian payment systems has been phenomenal, creating new records with each passing day. Digital payments volume in

India increased at a compounded annual growth rate of over 55 per cent in the past five years from 5.9 billion in 2015-16 to 34.3 billion in 2019-20, almost six times in 5 years. Retail payment systems such as the UPI and Aadhaar Enabled Payment Service (AePS) have changed the entire dynamics of retail payment systems as they are being used at every nook and corner of the country.

Last year when many other nations were writing cheques to provide stimulus to the people, we, in India, processed 274 crore digital transactions to provide Direct Benefit Transfer (DBT) to the people straight into their bank accounts.

16. 24x7 and interoperability are two key aspects that are the hallmarks of our payment systems and it would continue to be so. Interoperability is sine-qua-non if the existing infrastructure has to be leveraged to its optimum use. RBI's recent initiative in setting-up a Payment Infrastructure Development Fund (PIDF) to expand the reach of digital payments infrastructure into less penetrated regions is aimed at making payments more inclusive.

The emphasis of the Reserve Bank is on operationalising all our payment systems round the clock, 365 days a year and I am happy to say that with 24x7 NEFT and RTGS systems, we are among a few countries that provide the facility to transfer any amount at any point of time.

17. The success of UPI in India has attracted immense admiration from the international community and several countries across the globe have expressed interest in developing a system on similar lines which could provide a basis for stronger bilateral business operations and economic partnerships.

The UPI system also has the potential to unfold into a cheaper and faster alternative to available means for multilateral cross-border payments as well. It would be appropriate to mention that our RTGS also has multi-currency capabilities and with 24x7 operations now, there is a scope to explore whether its foot-prints could be expanded beyond India.

With the Reserve Bank at the forefront of nurturing innovation, the day is not far, when we will experience cheaper, faster and safer cross border remittances. Also, the indigenous Rupay card network has shown astounding growth across strata and has a significant market share.

With Rupay having international presence, our home-grown card network could make a mark in the global financial landscape, going forward.

18. The Reserve Bank is intensively involved in developing an ecosystem, which would not only nurture the future technologies, but also stimulate the technological aspirations of the financial community.

On these lines, to enable the growth of FinTech in India, the Reserve Bank in August 2019 entered into the elite class of select few countries which have their very own regulatory sandbox ecosystem, where any regulated or unregulated entity can come and live test their innovative products or services in a controlled environment.

This is a collaboration between the regulator, the innovators, the financial service providers and the end users (customers) which would ensure that Indian consumers continue to receive the best in class financial services.

The responses to the 1st Cohort on "Retail Payments" and the 2nd Cohort on "Cross Border Payments" were encouraging. Additionally, the Reserve Bank has also created our own Innovation Hub (RBIH). This hub will collaborate with financial sector institutions, technology industry and academic institutions for exchange of ideas and development of prototypes related to financial innovations.

The Bank for International Settlements (BIS) and several central banks have also set up such hubs to stay ahead of the curve in technology absorption.

19. While doing all these, we need to be watchful of the risks associated with certain technological innovations. That being said, while we are working on introducing a digital version of the fiat currency, the Reserve Bank is also assessing the financial stability implications of introducing such a Central Bank Digital Currency (CBDC).

As the underlying technology is still developing, we are exploring ways for a clear, safe and legally certain settlement finality, which is most crucial for a secure and efficient payment system. It also needs to be appreciated that there are not many practical instances of operationalisation of CBDC across the world; this calls for utmost precaution so that we can produce a safe and robust model.

20. Enhancing cyber resilience is another important aspect when it comes to digital innovations. As we are expanding our operating hours and allowing for increased access and increased interoperability, there are persisting threats of cyber-attacks to our systems. Experience shows that even the most efficient and protected systems can get compromised which could expose stakeholders to disproportionate risks.

The Reserve Bank is constantly creating awareness of such incidents and encouraging banks and non-banks to establish and maintain capabilities to avert such attacks. One must also know how to ring-fence such attacks when they occur and swiftly repair and restore the systems to normalcy. Cyber crisis proofing of systems by undertaking periodic tests as well as drills is essential.

21. With increased digitisation and development of FinTech, the traditional ways of credit evaluation are expected to be replaced by new-age credit evaluation methods that focus on a slew of non-financial and reliable transactional data. Many FinTech firms have already adopted such an approach but it is expected that in times to come, this may become more mainstream than remaining a niche. This will further facilitate the cause of financial inclusion.

At the same time, however, it throws up a host of new challenges in terms of concerns of data privacy, consent, and security. Ethical behaviour of stakeholders in the payments value chain is important to surmount these concerns. Ability of financial sector entities to respond to these challenges may become a key factor in the determination of their competitive advantage.

*Concluding observations*

22. In the dynamic world of financial services, and more so after the pandemic, FinTech is expected to challenge the financial sector with innovations and its exponential growth. Harnessing FinTech for customer services will effectively control costs and expand the banking and non-banking businesses.

The increased use of digital payments brought about by COVID-19 could fuel a rise in digital lending in the current decade as companies accumulate consumer data and enhance credit analytics.

This in turn presents new and complex trade-offs between financial stability, competition and data protection; thereby, warranting new regulatory frameworks and novel ways of monitoring. It is imperative for the financial sector regulators to monitor global developments and formulate policy responses to the risks and the opportunities.

23. Going forward, banks need to address the financing needs of new sunrise sectors without undermining the traditional sectors of the economy. This conclave gives us an opportunity to look back on what has been accomplished and deliberate on what still needs to be done.

I wish to reiterate that we at the Reserve Bank are fully committed to use all our policy tools to secure a robust recovery of the economy from the debilitating effects of the pandemic.

The Reserve Bank remains devoted to build an enabling environment to develop the financial sector and create necessary preconditions for growth while preserving financial stability.

*Number 9*

## EIOPA consults on revised Guidelines on the use of the Legal Entity Identifier

The European Insurance and Occupational Pensions Authority (EIOPA) launched today a consultation on revised Guidelines on the use of the Legal Entity Identifier (LEI). LEI is now widely used by the financial industry especially in the European Union, not only for identification of legal entities but also for data quality purposes, supporting activities in the area of financial stability, oversight and supervision as well as consumer protection.

Following the introduction of LEI in 2012, EIOPA issued its own Guidelines on the use of the LEI in October 2014. EIOPA identified a need to review and subsequently revise its current Guidelines due to several reasons:

- EIOPA's strategy on data and digitalisation, including aim to increase data standardisation, and ongoing implementation of cross-cutting projects within EIOPA where data quality and assessment of interconnectedness is key;

- Reflection of the principle of proportionality;

- 2020 ESRB Recommendations on identifying legal entities which are focusing on the LEI as a common identifier;

- 2019 FSB Thematic Review on Implementation of the LEI which listed some remaining obstacles which prevented wider LEI adoption.

The focus of this public consultation refer to the scope (and its clarity) of entities that should have a Legal Entity Identifier. The suggested scope is broader than before. Apart from Institutions for Occupational Retirement Provision (IORPs) and insurance and reinsurance undertakings the context of branches and intermediaries is introduced.

The revised Guidelines also consider the need for a better and wider identification of groups of entities as well as third country branches. The revised Guidelines also cover the necessity to use LEI code for identification purposes when competent authorities report to EIOPA.

EIOPA is also seeking to feedback from stakeholders regarding the impact assessment in particular on proportionality aspects when it comes to IORPs

and intermediaries. All interested stakeholders are invited to provide comments by 30 June 2021.

## Table of Contents



To read more:
https://www.eiopa.europa.eu/content/consultation-proposal-revised-guidelines-use-of-legal-entity-identifier-lei_en

*Number 10*

## Recent Cyber Events: Considerations for Military and National Security Decision Makers

This recurring report is the collaborative view of NATO CCDCOE researchers highlighting the potential effects of current events and developments in cyberspace on armed forces, national security and critical infrastructure, based on publicly available information.

It does not set out to be exhaustive. While the authors have made every effort to describe events from a perspective relevant to NATO and partner nations, there may be national and regional differences which this paper does not address.

The authors of this paper are independent researchers at the NATO CCDCOE; they do not represent NATO, nor does this paper reflect NATO's position. The aim of the paper is not to replace information about vulnerabilities and incidents provided by CSIRTs and providers of CIS products and services.

*Social engineering campaign against security researchers*

Social engineering is one of the oldest methods of influencing and manipulating people. In a general sense, it is the 'management of human beings in accordance with their place and function in society.

In the information environment, social engineering is defined as 'the use of fraud to manipulate individuals in the disclosure of confidential or personal information that may be used for fraudulent purposes.

Social engineering uses various techniques and tactics to influence, mislead and deceive targets. Hence, fraud can be purely digital or Social engineering uses various techniques and tactics to influence, mislead and deceive targets. Hence, fraud can be purely digital or analogue, or a combination of offline and online actions taken to deceive or compromise individuals, groups or organisations.

Some of the most common forms of digital social engineering are phishing, spear-phishing, mass phishing, vising (phone calls), fake news, market manipulation, political sabotage, scareware and baiting. To read more: https://ccdcoe.org/uploads/2021/03/Recent-Cyber-Events-No9_March_2021_Final.pdf

## 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.

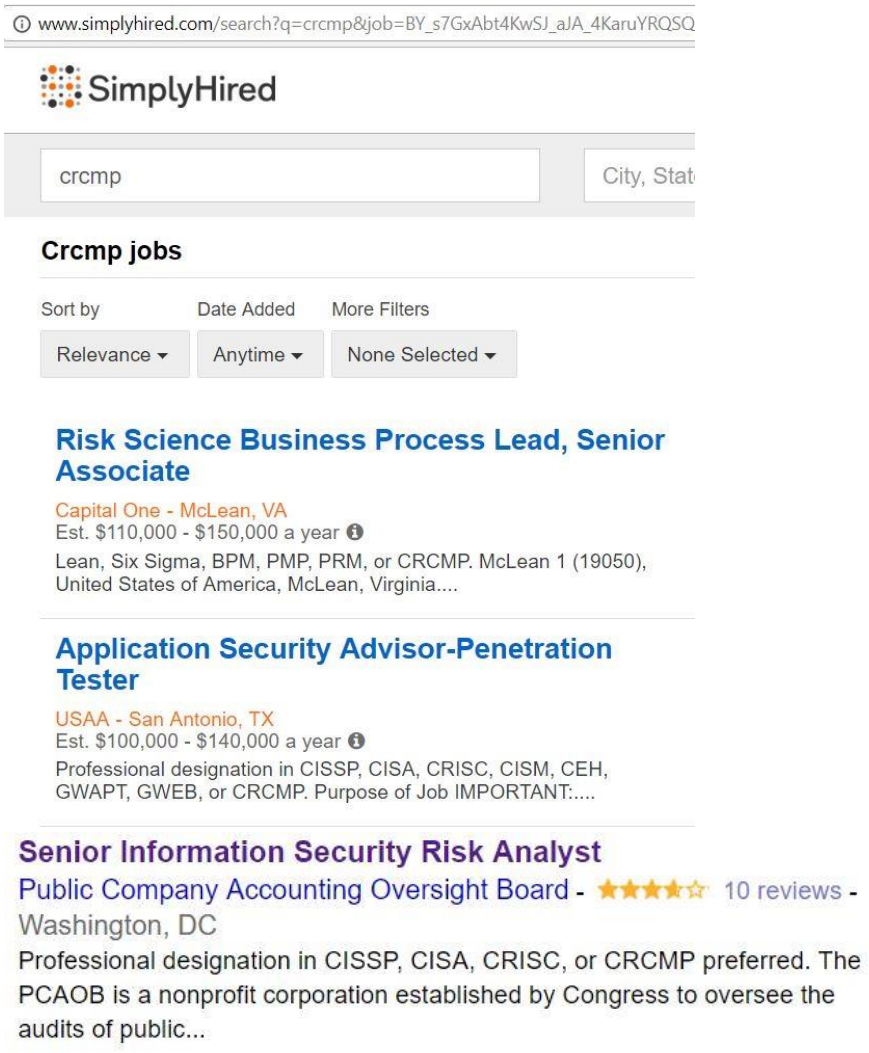
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

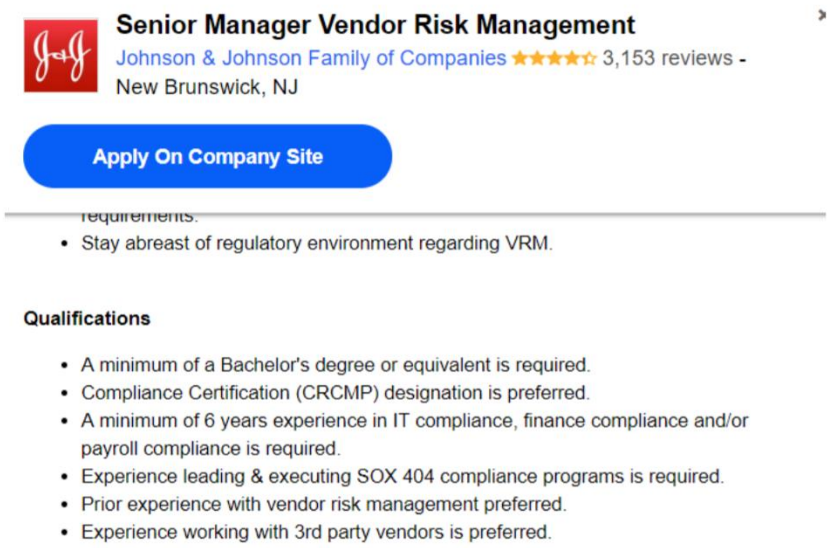
You can explore what we offer to our members:

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.