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, November 29, 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,

A cyber-attack on a technology company that provides services to financial institutions – or their service providers – could spread to the financial system. A *high concentration* of third-party service providers could magnify this risk.

This is part of the *2021 FSB Annual Report*. You must read this document.

We also read that while outsourcing to third-party providers, such as cloud services, may have enhanced operational resilience at financial institutions, *increased reliance* on such services can give rise to new challenges and vulnerabilities.

Financial institutions have relied on outsourcing and other third-party relationships for decades. However, in recent years, the *extent and nature* of interactions with a broad and diverse ecosystem of third parties has evolved, particularly on technology.

The FSB has analysed regulatory and supervisory issues associated with financial institutions' reliance on third-party providers. Identified challenges include the *design of contractual agreements* with third parties on appropriate rights to access, audit and obtain information from third parties; management of sub-contractors and supply chains; and the possibility of *systemic risk* arising from concentration in the provision of some outsourced and third-party services to financial institutions.

In light of the feedback received from external stakeholders, the FSB is launching further work to develop common definitions and terminologies related to *third-party risk management and outsourcing*, as well as expectations for financial authorities' oversight of financial institutions' reliance on critical service providers.

We can also read that cyber incidents are becoming more frequent and sophisticated. A cyber-attack that severely impairs the operational capability of a *systemically important* financial institution or critical part of the market infrastructure could spill over to other financial institutions, including as a result of a loss of confidence in the financial system.

Rapidly evolving crypto-asset markets may give rise to new risks to financial stability. Crypto-assets represent a small proportion of financial assets and are not widely used in critical financial services on which the real economy depends. However, their market capitalisation has increased dramatically and they have been used more by institutional investors, including in complex investment strategies.

Links between crypto-assets and the mainstream financial system through trading platforms and custodial services are also growing.

Increased participation by retail investors in speculative crypto-asset trading, facilitated by the use of so-called stablecoins, could also give rise to broader financial stability issues through an erosion of trust in the financial system.

So-called "global stablecoins" (GSCs) may also create vulnerabilities if adopted widely. Yet, despite an increase in the use of existing stablecoin arrangements in the past year, the functions they perform remain limited.

They are typically a by-product of demand for, and investments in, speculative crypto-assets, and are not yet being used for mainstream payments on a significant scale. However, one or more of them may evolve over time and could have the potential to expand reach and adoption across multiple jurisdictions, posing greater risks to financial stability than existing stablecoins.

We can also read that in an environment of high uncertainty, the potential for sudden sharp movements in asset prices persists.

In a context of persistent low interest rates, there is continued evidence of elevated risk taking among investors, which may add to existing vulnerabilities. The proportion of high-yield bonds outstanding is high and the amount of collateralised loan obligations remains high relative to the total amount of corporate debt. There are also signs of *higher leverage* being used in some markets, which could amplify market corrections.

You can read more at number 2 below. Welcome to our Top 10 list.

Best regards,

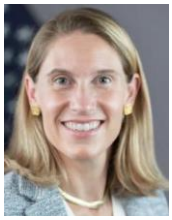
George Lekatis
President of the IARCP
1200 G Street NW Suite 800,
Washington DC 20005, USA
Tel: (202) 449-9750
Email: lekatis@risk-compliance-association.com
Web: www.risk-compliance-association.com
HQ: 1220 N. Market Street Suite 804,
Wilmington DE 19801, USA
Tel: (302) 342-8828

Stability Conference, cohosted by the Federal Reserve Bank of Cleveland and the Office of Financial Research, Cleveland, Ohio

Number 7 (Page 28)

Controlling Internal Controls

Remarks at the PepsiCo-PwC CPE Conference, SEC Commissioner Caroline A. Crenshaw



Number 8 (Page 31)

Deepening trust, reinforcing cooperation

Burkhard Balz, Member of the Executive Board of the Deutsche Bundesbank, to mark the inauguration of the Bundesbank's new representative in Rome.

Number 9 (Page 35)

EIOPA publishes annual occupational pensions statistics

eiopa
European Insurance and Occupational Pensions Authority

Number 10 (Page 37)

NIST Seeks Public Input on Consumer Software Labeling for Cybersecurity

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

Number 1

The "Secure Equipment Act of 2021".

CONGRESS.GOV

One Hundred Seventeenth Congress
of the
United States of America

AT THE FIRST SESSION
Begun and held at the City of Washington on Monday,
the fourth day of January, two thousand and twenty-one

An Act

To ensure that the Federal Communications Commission prohibits authorization of radio frequency devices that pose a national security risk.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Secure Equipment Act of 2021".

SECTION 1. SHORT TITLE.

This Act may be cited as the "Secure Equipment Act of 2021".

SEC. 2. UPDATES TO EQUIPMENT AUTHORIZATION PROCESS OF FEDERAL COMMUNICATIONS COMMISSION.

(a) RULEMAKING.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the Commission shall adopt rules in the proceeding initiated in the Notice of Proposed Rulemaking in the matter of Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program (ET Docket No. 21–232; FCC 21–73; adopted June 17, 2021), in accordance with paragraph (2), to update the equipment authorization procedures of the Commission.

(2) UPDATES REQUIRED.—In the rules adopted under paragraph (1), the Commission shall clarify that the Commission will no longer review or approve any application for equipment authorization for equipment that is on the list of covered communications equipment or services published by the Commission under section 2(a) of the Secure and Trusted Communications Networks Act of 2019 (47 U.S.C. 1601(a)).

(3) APPLICABILITY.—

(A) IN GENERAL.—In the rules adopted under paragraph (1), the Commission may not provide for review or revocation of any equipment authorization granted before the date on which such rules are adopted on the basis of the equipment being on the list described in paragraph (2).

(B) RULE OF CONSTRUCTION.—Nothing in this section may be construed to prohibit the Commission, other than in the rules adopted under paragraph (1), from—

(i) examining the necessity of review or revocation of any equipment authorization on the basis of the equipment being on the list described in paragraph (2); or

(ii) adopting rules providing for any such review or revocation.
The Act:
https://www.congress.gov/117/bills/hr3919/BILLS-117hr3919enr.pdf

One Hundred Seventeenth Congress
of the
United States of America

AT THE FIRST SESSION

Begun and held at the City of Washington on Monday, the fourth day of January, two thousand and twenty-one

An Act

To ensure that the Federal Communications Commission prohibits authorization of radio frequency devices that pose a national security risk.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Secure Equipment Act of 2021".

Number 2

2021 FSB Annual Report

FSB FINANCIAL STABILITY BOARD

Executive summary

The outlook for financial stability continues to be dominated by the COVID event.

- The G20 reforms and a swift and broad-based policy response to the pandemic were key to stabilising the financial system and sustaining financing to the real economy.

- The global economy is recovering from the fallout of the pandemic, supported by easy financing conditions. But the recovery is uneven across economies and sectors.

The combination of pronounced economic uncertainty, easy financing conditions and sustained policy support is shaping asset valuations, and could test financial resilience.

- Asset valuations may be stretched in some segments. Given high uncertainty, the potential for sudden sharp movements in asset prices persists, and could be associated with heightened liquidity demands that lead to spillovers across the financial system.

- The economic impact of the pandemic and of policy responses to address it have led to a rise in indebtedness across sovereigns, non-financial corporates and households. There is a risk of higher insolvencies and credit losses as policy support is unwound.

- Different scenarios, such as a rapid tightening in financial conditions following a strong bounce-back in the global economy or a strong resurgence of the pandemic leading to another round of strict lockdowns, could trigger these financial vulnerabilities.

Structural changes are also affecting the nature of vulnerabilities in the financial system.

- Non-bank financial intermediation (NBFI) has grown considerably since 2008 and become more diverse and interconnected. NBFI's increasing importance for the real economy means that market liquidity has become more central to financial resilience.

- Accelerated digitalisation has improved efficiencies but also put the spotlight on operational resilience, including cyber risks that are becoming more frequent and sophisticated. Rapidly evolving crypto-asset markets may give rise to new risks to financial stability.

- Exposure to the physical and transition risks posed by climate change is a pressing emerging vulnerability. Climate-related events could lead to sharp changes in asset prices, and be concentrated in certain sectors or geographies. A disorderly transition to a low-carbon economy could have a destabilising effect on the financial system.

The FSB is carrying out analytical and policy work to foster global financial stability in response to the pandemic as well as to new and emerging risks, including:

- Work to enhance the resilience of the NBFI sector while preserving its benefits, building on the lessons from the March 2020 market turmoil. A key deliverable for this year is policy proposals to enhance the resilience of money market funds (MMFs).

- Work on regulatory and supervisory issues associated with financial institutions' reliance on third-party providers; cyber incident response and recovery; and to address specific risks arising from so-called "global stablecoin" arrangements.

- Analytical work on central counterparty (CCP) financial resources, given the increased shift to central clearing that has further increased the systemic importance of CCPs.

- The development of a roadmap to enhance cross-border payments, including the setting of quantitative global targets for cost, speed, transparency and access.

- Actions to promote the timely transition away from LIBOR to robust alternative rates.

- Work to assess and address climate-related financial risks, including the development of a roadmap to support internationally coordinated actions in this area.

There has been limited additional progress in implementing G20 reforms since last year, as financial authorities focused on responding to the impacts of the pandemic.

- Regulatory adoption of core Basel III elements has generally been timely to date, but implementation of the final reforms to the capital framework is still at a very early stage. Implementation of over-the-counter (OTC) derivatives reforms is also well advanced.

- More work is needed to close gaps in the operationalisation of resolution plans for banks and to implement effective resolution regimes for insurers and CCPs. The implementation of NBFI reforms continues but is at an earlier stage than other reforms.

The pandemic provides important lessons for the functioning of the G20 reforms.

- Effective implementation of those reforms meant that core parts of the financial system entered the pandemic in a more resilient state than during the 2008 crisis. Those parts of the system where implementation is most advanced displayed greater resilience and were able to cushion, rather than amplify, the shock.

- The pandemic highlighted differences in resilience within and across financial sectors, and areas that warrant further consideration at the international level. These include the functioning of capital and liquidity buffers; factors that may give rise to excessive procyclicality in the financial system; and the need to strengthen NBFI resilience. The FSB, working with SSBs, is examining the policy implications of these findings.

The COVID experience reinforces the importance of global regulatory cooperation and of completing the remaining elements of the post-crisis reform agenda with G20 support.

- The financial stability benefits of the full, timely and consistent implementation of G20 reforms remain as relevant as when they were initially agreed.

- Maintaining close monitoring and cooperation are critical given the impacts of the pandemic and the need to support the resilience of the global financial system and address long-term structural developments in the financial system.

- The FSB and SSBs will continue to promote approaches to deepen international cooperation, coordination and information-sharing, with the support of the G20.

To read more: https://www.fsb.org/wp-content/uploads/P271021.pdf

Number 3

Cybersecurity Spending: An analysis of Investment Dynamics within the EU

The European Union Agency for Cybersecurity issues a new report on how cybersecurity investments have developed under the provisions of the NIS directive.

In 2020, ENISA published its first report on network and information systems (NIS) investments in an attempt to collect data on how Operators of Essential Services (OES) and Digital Service Providers (DSP) identified in the European Union's directive on security of network and information systems (NIS Directive) invest their cybersecurity budgets and how this investment has been influenced by the NIS Directive.

This report is a follow-up covering all 27 EU Member States and offering additional insights into the allocation of NIS budgets of OES/DSP, the economic impact of cybersecurity incidents and the organisation of cybersecurity in these operators.

In addition, global cybersecurity market trends are presented through Gartner security data and insights observed globally and in the EU, in order to provide a better understanding of the relevant dynamics.

Data was collected through a survey of 947 organisations identified as OES/DSP across the 27 Member States.

In this second edition of the report, besides covering all Member States, additional and complementary questions were asked to the surveyed organisations.

Overall, 48.9 % of surveyed organisations acknowledge a very significant or significant impact of the NIS Directive on their information security (IS).

Other key findings of this report are as follows.

- Almost 50 % of the established OES/DSP within the EU believe that implementing the NIS Directive has strengthened their detection capabilities, while 26 % believe that it has strengthened their ability to recover from incidents.

- 67 % of OES/DSP required a dedicated budget for the NIS Directive implementation, with a median value of EUR 40 000 or 5.1 % of their overall information security budgets. Around 50 % of organisations required on median four additional full-time employees (FTEs) for the implementation, either via recruitment or outsourcing.

- The estimated direct cost of a major security incident is EUR 100 000 on median, with the banking and healthcare sectors experiencing the highest such costs of EUR 300 000 and EUR 213 000 respectively. The primary cost factors for this figure include costs related to revenue losses and data recovery or business continuity management. 9 % of organisations have suffered a major security incident that impacted external stakeholders.

- In 28 % of the surveyed OES/DSP, the Chief Information Officer (CIO) or Chief Technology Officer (CTO) is responsible for information security while in over 50 % of cases, the Head of Information Security reports directly to the Chief Executive Officer (CEO), the Board of Directors (BOD) or the President.

- More than 50 % of the surveyed OES/DSP do not possess any form of cyber insurance, but around 25 % are planning to obtain coverage.

- More than 50 % of the surveyed OES/DSP certify their systems and processes.

- The majority of the surveyed OES/DSP report that their information security controls meet or exceed industry standards, with only 5 % reporting that they do not meet those standards.

- The results indicate a strong correlation between a very positive self-perception of cybersecurity maturity and the existence of cybersecurity certifications for processes, people and products within an organisation.

Table 1: Categories of OES/DSP as defined in the NIS Directive

Categories of OES and DSPs	
OES	**DSPs**
• Energy (electricity, oil and gas) • Transport (air, rail, water and road) • Banking • Financial market infrastructures • Health • Drinking water supply and distribution • Digital infrastructure	• Online marketplace • Online search engine • Cloud computing service

Figure 10: The information security skills landscape dynamics

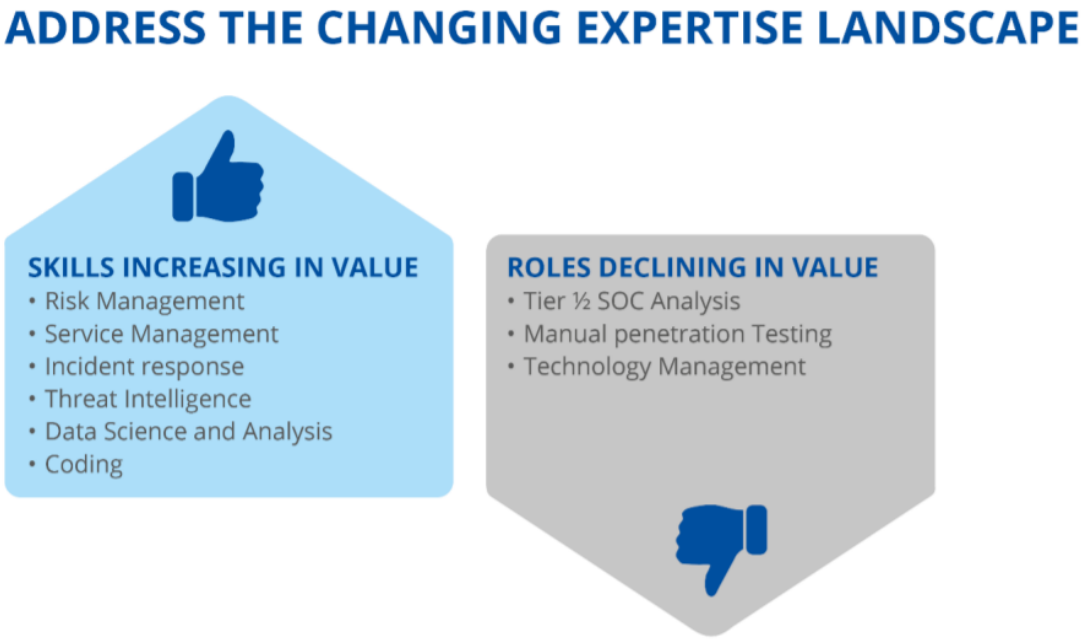
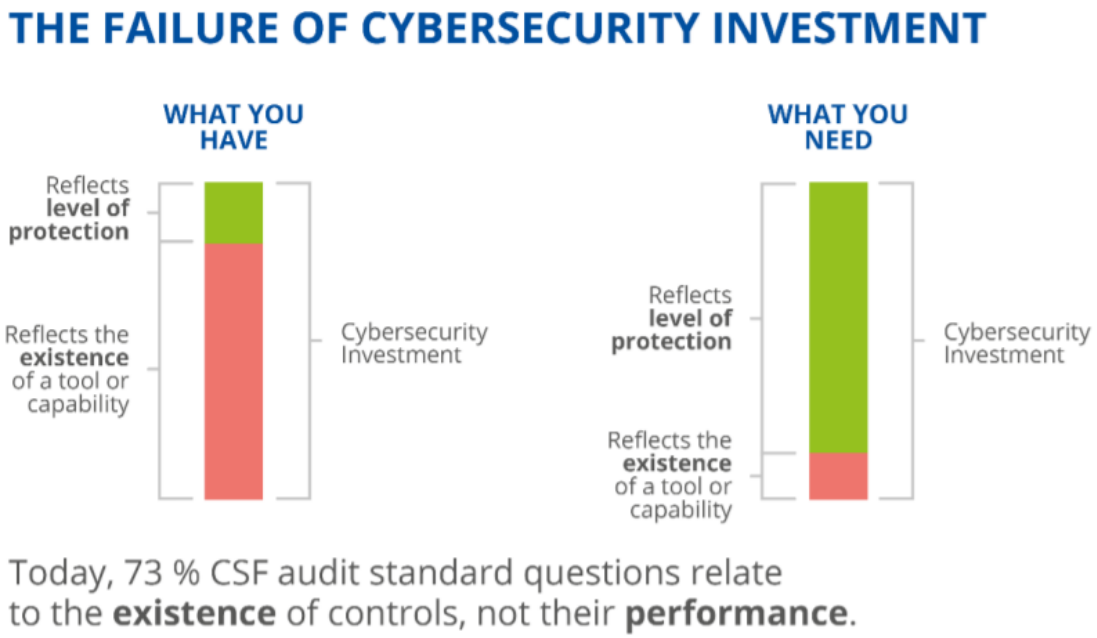


Figure 12: Cybersecurity controls – existence vs performance



You may visit:
https://www.enisa.europa.eu/publications/nis-investments-2021

Number 4

Central Banks and Climate: not the only game in town, but more committed than ever

François Villeroy de Galhau, Governor of the Banque de France, Climate Finance Day – Paris, 26th October 2021

Ladies and Gentlemen,

It is always a pleasure to attend this landmark event for sustainable finance. But on the eve of COP 26 opening, climate emergency is such that I owe you more than just another speech.

I see it as my duty both to report the great progress we have made in this area and to set out the enormous challenges that lie ahead: in very concrete and practical terms, what we have achieved since the last Climate Finance Day in October 2020 (I), and what we have to further achieve in the coming year, notably on a better understanding of the macroeconomic effects of climate change (II).

I. Our climate action has accelerated over the past year

I am proud to stress that the Banque de France, and more generally Central banks have never been more committed.

Addressing climate change is part of our missions as supervisor and Central bank: we are acting in the very name of our mandates. Our actions revolve along two axes, as stylised in this quadrant.

Against the vertical axis, as **supervisors**, we have made significant progress to identify and help contain climate-related **risks** born by financial institutions.

The ACPR took a decisive step forward with the very first climate related stress tests, whose results were published in May 2021.

A large number of major banks and insurance companies took part on a voluntary basis. The two key takeaways from this pilot exercise are that

(i) financial risks are better contained in the context of an early and orderly transition to a greener economy,

(ii) all main supervisors should now follow suit, as for instance the ECB and the Bank of England will in spring 2022.

When it comes to climate stress tests, learning by doing is much better than waiting for the perfect solution before taking any action.

On voluntary disclosure of risks, the TCFD increased its footprint; it now has more than 2,600 supporters (a number that has more than doubled since last year), including more than 50 central banks.

The European Union is about to make a significant step forward, as it will implement mandatory disclosure for corporates through a new standard developed by the EFRAG with the Corporate Sustainability Reporting Directive (CSRD), which should hopefully be adopted by mid-2022.

Some might always argue – passionately – that Europe and France never do enough.

Yes we must do more but we should value the reality of action to rhetorical over-bidding. We must avoid discouraging those who are doing the most while excusing those who do the least.

I very much hope we will soon have this mandatory disclosure everywhere.

I welcome the US endeavour here under the sponsorship of the SEC.

Ultimately we need internationally harmonised disclosure frameworks – at least a basic common ground on which jurisdictions can further elaborate.

To this end, interoperability of standards will be key, and the coordination between the EFRAG and the IFRS Foundation, should be the cornerstone of a successful globalisation of non-financial reporting standards.

On financial opportunities (let me turn now to the lower part of the axis), the market momentum has been impressive this year again.

More than half a trillion USD of green bonds will be issued this year, which is an all-time high, with record debut for the EUR 12 bn NextGeneration EU green bond.

Inflows into sustainable funds represented more than USD 262bn in the first half of this year, close to half of the overall inflows (USD 545bn) over the same period.

On the horizontal axis, which brings together our missions as a Central bank, we collectively achieved a major breakthrough last July with the conclusion of the ECB monetary policy strategy review under Christine Lagarde's leadership.

The Banque de France contributed decisively.

The ECB is pioneer in having decided an ambitious action plan by 2024, including the three following steps:

(1) make economic projections, and therefore model. This dimension of economic research is often overlooked: it is nevertheless crucial to grasp complex interdependencies between physical and economic phenomena, across sectors and countries, and across time horizons – I will come back to it;

(2) disclose: impose transparency requirements including on counterparties;

(3) incorporate climate risk, into our operations on corporates (on both asset purchases and collateral policies).

As regards asset purchases, the CSPP should take into account climate-related factors, including the alignment of issuers with the Paris agreement, and will adjust purchases on the primary and secondary markets accordingly.

Moreover, regarding euro-denominated non-monetary portfolios, Eurosystem central banks committed last February to implement sustainable and responsible investment strategies and to report the first results by end of 2022.

Banque de France's policy has been exemplary since 2018 regarding the management of its own funds, whose alignment on a 2° C objective is already effective.

We won't stop there though: we started to exit from non-conventional oil and gas earlier this year, we announced that we are exiting totally from coal by end 2024. We now commit to work toward aligning our own portfolios with a 1.5°C objective.

One additional word about the international context of these developments. Here again, we saw a major improvement this last year with the new American involvement: climate-related issues are now firmly on the agenda of the G20, the G7, the FSB and all other standard setting bodies.

The NGFS, created in Paris in December 2017, is a unique knowledge hub. It now has 95 members, including the US Fed since last December and this number will still grow in coming weeks.

The Banque de France provides its global secretariat with 15 staff, and we created last April our Climate Change Centre chaired by Nathalie Aufauvre.

We are indeed making good progress across the board. But each year that passes without sufficient emission reductions makes the issue more severe, and the solutions more radical.

To grapple with this dynamic situation, it is imperative that we are able to better understand and forecast the macroeconomic impacts of climate developments.

2. An imperative for the year to come: forge models that gauge the interaction between climate and the economy

One aspect of the ECB's action plan launched on the back of the strategy review may have received too little attention: macroeconomic modelling and scenario analyses.

The challenge is huge as we face a triple source of uncertainty: first, how climate change will materialise, second, what the transition could look like and, third, how both will translate to the macroeconomy.

The NGFS has produced detailed macro financial scenarios and the corresponding data that provide the most comprehensive framework to date for financial risk assessment.

To make such scenarios possible, the central banking community – with a strong involvement of Bank of England and Banque de France among others - has collaborated with first tier research institutes in climate science and economic modelling.

This is a huge step forward. Our objective is now to propose a common set of plausible and differentiated futures, built with the best available science and anchored in the last available IPCC results.

Each jurisdiction or region will use them as they want, for their own stress tests and economic simulations, but there is no reason to base them on alternative set of scenarios.

The purpose of the NGFS is to prepare and publish these common macro financial climate scenarios, just as the IPCC does for physical scenarios.

Having this common language, instead of numerous local ones, will make our international discussion much easier. To this end, we are considering several significant steps forward.

By next summer, the NGFS scenarios will not only be updated with the latest figures, but also upgraded to align with the new set of comprehensive scenarios to be released in March by the IPCC and to incorporate the more extreme ones.

The NGFS should also work on understanding the impact of climate-related risks on various prices and ultimately on overall inflation.

Scanning the horizon, we can already see that climate change is accelerating, and that some regions are likely to be affected sooner and on a larger scale.

In addition, transition effects might be more front-loaded as they are increasingly anticipated by markets, producers and consumers, which would be good news.

The forthcoming NGFS work should therefore also focus on shorter-term horizons (2030, and not only 2050) as the transition to a low-carbon economy may be less linear than anticipated, with tipping points accelerating the transition in a disorderly way.

[Slide] We generally need to better understand the long-term trade-off, in terms of GDP, between transition and physical risks and the cost of delayed action.

The chart breaks down the GDP losses under three scenarios into the costs of transition and physical damages.

Under the “Paris Agreement” scenario, GDP would be 5% lower in 2060 and around 7% lower in 2100, and most of this reduction can be attributed to transition policies.

Under the two “Too-little too-late” scenarios, the transition costs are limited, but by the end of the century the impact of physical risks becomes much larger, leading to overall losses that could range between at least 10 and 20% of world GDP level.

From an economic and rational standpoint, the prescription is clear-cut: an orderly transition would require a governmental forward-looking guidance, sending long-term signals and anchoring credible but ambitious commitments.

This “climate forward guidance” should include an appropriate pricing of carbon; and as long as we don’t have such global pricing, a carbon border adjustment mechanism (CBAM), as recently put forth by the EU in order to prevent carbon leakage is appropriate.

We all know how politically sensitive these issues are, domestically as well as internationally. But the political scene on climate has already been changing dramatically and it will continue to change - hopefully for the better.

Looking back at how far we have come in developing green finance over the last six years, one may wonder: “Is it useful?” – certainly yes; “Is it enough?” –certainly not.

Let me remind everyone of one simple – and dreadful number: according to the IPCC, we have less than six years of greenhouse gases budget left if we want to have 83% chance to stay below 1.5°C.

Let’s not fool ourselves: we have been making very significant progress to make sure that the financial system is fit to the challenge of the transition. But there is still much work to do on our side, starting with mandatory and harmonised disclosures, and a close monitoring of transition paths.

Still more fundamentally, what we are doing only makes sense if this is part of a wider collective endeavour. Finance, and still more Central banks, cannot be the only green game in town.

A few days ahead of Glasgow, it is the right time to listen to the Pink Floyd again and the Dark Side of the Moon: “And then one day you find ten years have got behind you; no one told you when to run, you missed the starting gun”4. It is not too late yet, but let us hear the starting guns. I thank you for your attention.

To read more:
https://www.banque-france.fr/sites/default/files/medias/documents/discours_20211026_climate-finance-day_en.pdf

Number 5

Irving Fisher Committee on Central Bank Statistics

IFC Bulletin No 55 - New developments in central bank statistics around the world

BANK FOR INTERNATIONAL SETTLEMENTS

New developments in official statistics – A central banking perspective after Covid-19, Alfonso Rosolia, Silke Stapel-Weber and Bruno Tissot

Executive summary

The experience of central banks has underlined the potential of alternative data sets to deliver statistics that are higher-frequency as well as more timely, flexible and granular than traditional ones.

These are urgently needed to help policymakers follow macroeconomic developments and support policy decisions.

In particular, the new, unconventional sources of information that have emerged with the digital transformation of our societies show a lot of promise (Hammer et al (2017)).

They can cover many realms of the economic and financial sphere that are still difficult to capture through more traditional data collections. And they are potentially available in near real time, facilitating the conduct of economic policy especially in the face of unexpected shocks.

Yet these new data sources can come with huge numbers, multiple formats and high noise-to-signal ratios, making them difficult to use systematically in policymaking and statistical production.

Some of these challenges might be addressed with appropriate engagement rules between public agencies and private data providers; others require further adequate improvement in our statistical and analytical methodological work.

Meeting all these challenges will make life easier for the statistical and policymaking communities.

It's worth noting here that what may at first sight look like an information gap does not necessarily reflect a lack of relevant data, but rather a failure to transform existing indicators into useful knowledge (Drozdova (2017)).

This is even more the case in today's evolving information society: torrents of data are constantly generated, collected and stored by both public and private agents.

This means that perceived information gaps do not necessarily require new reporting exercises, as they may arguably be filled if statisticians and policymakers can quickly tap into existing data that could be turned into useful information, for instance to get timelier or higher-frequency measures of common phenomena or to cover new, unexplored statistical domains.

Introduction

Central banks have an almost unique perspective on official statistics, being at the forefront of both the production and the application of economic and financial data.

On the one hand, they produce statistics on a wide variety of domains, especially the financial system, that are of key relevance for a broad range of economic policymakers.

On the other hand, central banks make extensive use of diverse data sources in pursuing their objectives, especially their monetary policy and financial stability goals.

Both roles demand constant attention to the economic and financial environment and the fitness-for-purpose of statistics and analytical tools and products.

A key challenge is that this environment is constantly changing, which requires the official statistical framework to evolve continuously.

In Japan, for instance, digitalisation has brought new types of service (eg internet advertising) that need to be considered when measuring inflation; this has also called for the development of new types of statistical method at the Bank of Japan, eg to adjust for quality changes.

Moreover, while available statistical products and methods are designed to describe what is known to be relevant to decision-makers, this knowledge is not fixed in time, since new policy issues constantly emerge.

These discontinuities in both the supply of statistics and the demand for them can be substantial, especially when large and unusual shocks occur that expose gaps in economic and financial information.

The vulnerabilities underlying the 2007–09 Great Financial Crisis (GFC), for example, went almost unnoticed by policymakers at first because of the lack of suitable statistics.

However, through swift and globally coordinated action, the most critical data gaps were singled out and action plans designed to address them, especially via the Data Gaps Initiative (DGI) endorsed by the G20 (FSB and IMF (2009)).

In the decade or so since the GFC, extensive work has been done to close the most pressing data gaps and strengthen the ability to monitor global economic financial developments.

These improvements proved their worth when the pandemic struck: policymakers had at their disposal statistics of a quality and variety that would have been barely possible a few years ago (IFC (2021b)).

The potential of this new information for monitoring risks in the financial and non-financial sector as well as for the analysis of interconnectedness and cross-border spillovers was underlined during the Covid-induced financial markets turmoil in March 2020 (FSB (2020)).

New lessons have emerged from the pandemic. One is the sheer speed of developments during a crisis, underlining the importance of high-frequency, well documented and timely indicators to support evidence-based policy.

This calls for statistical frameworks to become more flexible and granular with the aim of addressing the evolving needs of users and help them monitor fragilities (De Beer and Tissot (2020)).

Another lesson is that the (unexpected) nature of the shock has clearly expanded the range of statistics that central banks must look at.

The unpredictability of the data needs that arise when a shock hits the economy means that instruments and arrangements are needed for the key phenomena to be measured as soon as they become relevant.

A third lesson is that the disruptions caused to the traditional statistical production process, for example, due to the suspension of key surveys, have highlighted the need to look at less conventional and still untapped sources of alternative information (Biancotti et al (2021)).

To read more (506 pages) you may visit:
https://www.bis.org/ifc/publ/ifcb55.pdf

Number 6

Reflections on Stablecoins and Payments Innovations

Christopher J. Waller, Member Board of Governors of the Federal Reserve System, at "Planning for Surprises, Learning from Crises" - 2021 Financial Stability Conference, cohosted by the Federal Reserve Bank of Cleveland and the Office of Financial Research, Cleveland, Ohio

The U.S. payment system is experiencing a technology-driven revolution.

Shifting consumer preferences and the introduction of new products and services from a wide variety of new entities have led to advancements in payments technology.

This dynamic landscape has also sparked an active policy debate—about the risks these new developments pose, how regulators should address them, and whether the government should offer an alternative of its own.

Earlier this year, I spoke about the last of these questions: whether the Fed should offer a general-purpose central bank digital currency (CBDC) to the American public.

My skepticism about the need for a CBDC, which I still hold, comes in part from the real and rapid innovation taking place in payments.

My argument—simple as it sounds—is that payments innovation, and the competition it brings, is good for consumers.

The market and the public are telling us there is room for improvement in the U.S. payment system.

We should take that message to heart and provide a safe and sound way for those improvements to occur.

My remarks today focus on "stablecoins," the highest-profile example of a new and fast-growing payments technology.

Stablecoins are a type of digital asset designed to maintain a stable value relative to a national currency or other reference assets.

Stablecoins have piggybacked off the recent increase in crypto-asset activity, and their market capitalization has increased almost fivefold in just the past year.

Stablecoins can be thought of in two forms.

Some serve as a "safe, liquid" asset in the decentralized finance, or DeFi, world of crypto-trading.

Examples include Tether and USD Coin.

Alternatively, there are stablecoins that are intended to serve as an instrument for retail payments between consumers and firms.

Although these types of stablecoins have not taken off yet, some firms are working to assess the viability of such stablecoins as a retail payment instrument.

This growth in usage of stablecoins and their potential to serve as a retail payment instrument has prompted regulatory attention, including a new report from the President's Working Group on Financial Markets (PWG).

This report urges the Congress to limit the issuance of "payment stablecoins" to banks and other insured depository institutions.

Fostering responsible payments innovation means setting clear and appropriate rules of the road for everyone to follow.

We know how to handle that task, and we should tackle it head-on.

The PWG report lays out one path to responsible innovation, and I applaud that effort.

However, I also believe there may be others that better promote innovation and competition while still protecting consumers and addressing risks to financial stability.

This is the right time to debate such approaches, and it is important to get them right.

If we do not, these technologies may move to other jurisdictions—posing risks to U.S. markets that we will be much less able to manage.

Stablecoins: What's Old, and What's New

Stablecoin arrangements involve a range of legal and operational structures across a range of distributed ledger networks.

They are a genuinely new product, based on genuinely new technology. But despite the jargon surrounding stablecoins, we can also understand them as a new version of something older and more familiar: the bank deposit.

As I have said before, both the government and the private sector play indispensable roles in the U.S. monetary system.

The Federal Reserve offers both physical "central bank money" to the general public in the form of physical currency and digital "central bank money" to depository institutions in the form of digital accounts.

Commercial banks, in turn, give households and businesses access to "commercial bank money," crediting checking and savings accounts when a customer deposits cash or takes out a loan.

This privately created money serves as a bridge between the central bank and the public.

Commercial bank money is a form of private debt.

The bank issuing that debt promises to honor it at a fixed, one-to-one exchange rate with central bank money.

The bank itself is responsible for keeping that promise. However, the bank is supported in that task by a tried-and-true system of public support.

That includes regulation and supervision, which ensure banks are safe and sound, not taking imprudent risks in their day-to-day business; the availability of discount window credit, which ensures well capitalized banks can meet their emergency liquidity needs; and deposit insurance, which protects consumer deposits if the bank fails.

Put together, those programs leave very little residual risk that a depositor in good standing will ever have to leave the teller empty handed.

They make a bank's redemption promise credible, and they make commercial bank money a near-perfect substitute for cash.

As a result, households and businesses overwhelmingly use commercial bank money for everyday transactions.

This arrangement has many advantages. Small retail customers do not have to spend their time vetting the safety and soundness of their banks—regulators and supervisors do that for them.

Consumers have a safe place to keep their savings and a nearly risk-free way to make payments, which are settled in ultrasafe central bank liabilities.

Banks can focus their effort on investments, products, and services from a place of safety and soundness.

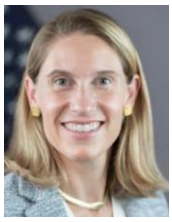
Communities and customers benefit from those efforts in the form of more efficient capital allocation and higher-quality, lower-cost financial products.

To read more:
https://www.federalreserve.gov/newsevents/speech/files/waller20211117a.pdf

Number 7

Controlling Internal Controls

Remarks at the PepsiCo-PwC CPE Conference, SEC Commissioner Caroline A. Crenshaw



Thank you for the kind introduction Kevin [Gould]. It's a pleasure to be here today at the annual PepsiCo-PwC CPE conference, which I understand is a tradition going back 18 years now. I appreciate the opportunity to speak, and I look forward to answering your questions today.

It's not often—even in this job—that I find myself speaking before such a large group of controllers, accountants and other finance professionals of public companies. And I welcome it because it means we can get a bit more technical and talk about financial reporting issues.

I suspect many of you will not be surprised that Kevin and his team have shared with me that ESG is top of mind for this group. I understand there is an interest in hearing what ESG means to the SEC and what ESG regulations are on the horizon. It's a big question, and spoiler alert – I cannot speak for the Commission and tell you what is to come.

I have to caveat my statements today with the standard disclaimer that any views I express today are my own and do not reflect the views of my fellow Commissioners, the Commission or its staff. But I am an U.S. Army reservist, and the Soldier in me truly appreciates your commitment to readiness. So even though I cannot speak for the Commission, today I will discuss how I have been thinking about ESG in the public issuer context.

I. ESG Risks Facing Today's Investors & Public Companies

ESG is not a monolithic concept. As you know, it generally refers to environmental, social and governance risks, and these are some of the most pressing issues companies are facing.

In March of this year, the Commission sought public comment on climate change disclosure.

We received hundreds of responses; many of which also addressed disclosures concerning other ESG risks.

An overwhelming number of comment letters state that investors view ESG information as material to financial performance and that investors need consistent and reliable disclosures of ESG information to inform their investment decisions.

According to commenters, ESG related information helps investors assess the long-term sustainability or value of an investment.

And this makes sense if you think about the position investors are in today. Many Americans are no longer able to rely on defined-benefit retirement plans.

They must, instead, rely on themselves in order to save for their children's education or for their own retirement. And they must, in doing so, take on the risks associated with managing the money themselves.

Investors increasingly need to consider how companies will "weather" over a longer time horizon when making investment decisions.

That requires looking at the risks today's companies face and analyzing how these risks will impact future financial performance.

With ESG now front and center, the reliability of corporate ESG risk disclosures, and their potential impact on and connectivity to financial statements, is critical. As you know, corporate internal controls play a crucial role in ensuring such risk disclosures are consistent and reliable.

The term "internal accounting controls" refers to an organization's plan, methods, and procedures related to safeguarding a company's assets and ensuring the reliability of corporate financial records.

These controls broadly include systems designed to ensure transactions are authorized and recorded in a way that maintains accountability for assets and allows for financial statement preparation in conformity with GAAP.

They also include procedures that control access to assets and the systems designed to test the effectiveness of internal controls.

The concept of accounting controls is intentionally broad, because a company's system for tracking its assets and recording transactions – regardless of their form – is vital to accurate financial reporting.

And it is vital to identifying risks to the financial statements so leadership can manage them and prepare GAAP-compliant financial statements and disclosures accordingly.

At the end of the day, management is responsible for establishing and maintaining an effective system of internal controls that reasonably safeguards corporate assets from risk.

So as you think about and discuss ESG risks during this conference, I encourage you to think about them in the context of your internal accounting controls and audit functions.

II. Internal Accounting Controls and ESG Risks

To best serve their function, internal accounting controls must be dynamic enough to consider and respond to changes in the markets, such as those posed by ESG issues.

Companies have to evolve over time because the market place is constantly changing in response to new developments and challenges.

These changes can be prompted by new technology, developments in the global economy, or even by our planet.

Change drives innovation for not just corporate America, but investors, consumers and citizens.

Change can be a good thing. But as markets change, so do the risks that can impact a company's financial statements.

Corporate internal accounting controls must evolve as well. Although these are relatively technical matters often thought of as within the remit of accounting and legal professionals of a specific company, I am regularly reminded that, in the aggregate, these details matter to all Americans.

These details impact the companies whose aggregate financial performance undergirds the retirement savings of tens of millions of workers, and retirees.

To read more:
https://www.sec.gov/news/speech/crenshaw-controlling-internal-controls-20211116

Number 8

Deepening trust, reinforcing cooperation

Burkhard Balz, Member of the Executive Board of the Deutsche Bundesbank, to mark the inauguration of the Bundesbank's new representative in Rome.

1 Introduction

Ladies and gentlemen,

Italy, and especially Rome, have always been destinations that many Germans have longed to visit.

One of these Germans was without doubt the famous writer Johann Wolfgang von Goethe. From 1786 to 1788, he fulfilled a lifelong dream by travelling through Italy.

The report on his travels, which he titled “Italian Journey”, became a best seller and remains to this day the embodiment of many Germans’ yearning for Italy.

By the way, the “Italian Journey” can also be found in my personal library.

Several days ago marked the anniversary of a milestone event on this journey: 235 years ago, in late October 1786, Goethe had been on his travels for almost two months when he laid eyes on Rome for the first time.

Overwhelmed, he wrote in his diary “Now, at last, I have arrived in the First City of the World!” Nowadays, it is far quicker and easier to travel to Rome. Nevertheless, every time I visit I am delighted to be in this exceptional cosmopolitan city.

Our reason for being gathered together today is not to celebrate the anniversary of Goethe’s Italian journey.

The occasion is just as gratifying, though: the inauguration of Dr. Elisabetta Fiorentino as the Bundesbank’s representative at the German Embassy in Rome.

2 Cooperation in the Eurosystem

Ladies and gentlemen,

Much has happened since Goethe's travels to Italy. But what has not changed is the special relationship between Germany and Italy, the deep bond between the two countries. Without this bond, European integration and our single currency, the euro, would not have become possible.

The Bundesbank also has a variety of connections with Italy. We have especially close ties with our colleagues at the Banca d'Italia.

We work together harmoniously in many areas and in many working groups of the Eurosystem. One example that goes beyond the usual level of cooperation concerns payment systems.

The Bundesbank and the Banca d'Italia, alongside the Banque de France, manage TARGET2, Europe's most important payment system.

Together with the Banco de España, the three central banks also operate the TARGET2 Securities (T2S) settlement platform.

In doing so, they are providing efficient and secure payment systems and ensuring that payments throughout Europe can be made smoothly.

One thing is for sure: the joint operation of complex systems such as these can only succeed if all parties trust one another and pull together at all times. And that's exactly what we're doing! In addition, we're working on making payment systems fit for the future.

Just last week, for example, experts from the Bundesbank and the Banca d'Italia came together to exchange ideas on the possibilities for settling securities in central bank money using innovative market solutions based on distributed ledger technology (DLT).

Ladies and gentlemen,

Payment systems are just one example of the especially close cooperation between Germany and Italy within the Eurosystem. For this reason, I am delighted that we are now sending a representative to the German Embassy in Rome to strengthen our ties even further.

This is because Europe and the Eurosystem are undoubtedly facing significant challenges.

First of all, we need to tackle the coronavirus pandemic and its fallout. How can we ensure a successful economic recovery? How do we roll back the emergency measures? And what structural changes will the pandemic bring about over the medium and long term?

Furthermore, we must continue to develop European Economic and Monetary Union. How do we deal with the sharp rise in public debt in the euro area? How can we reconcile the single monetary policy with different national fiscal and economic policies? Will we be able to strengthen the capital markets union and complete the banking union?

And, finally, we must grapple with the pressing issues surrounding the megatrends of demographic change, decarbonisation and digitalisation. Above all, digitalisation is making waves in the financial sector and presenting challenges to central banks like the Bundesbank and the Banca d'Italia.

What will the digital financial system of tomorrow be like? Who will play what roles within that system? And how will we make payments in the future? With cash? Book money? Digital money? Or with central bank digital currency?

As different as all of these questions are, they do have one thing in common: they all require a joint European response. In this regard, it is absolutely clear that the need for international exchange, consensus and collaboration will continue to grow.

For this reason, we at the Bundesbank believe that it is vital to redouble our efforts to foster contacts with both other central banks as well as, in particular, national authorities and financial institutions in the major euro area countries.

The representatives that we send to the German Embassies in Paris, Madrid and now also Rome, are there to expand our networks in those countries and build upon our existing relationships.

Their objective is to increase mutual trust and understanding. For the Bundesbank, this is a way of helping to promote collective solutions and reinforcing cooperation within the euro area.

Digital media may have helped us all to stay in touch during the coronavirus pandemic – in fact, it worked much better than we'd initially anticipated. But one thing was clear in spite of all the digital tools at our disposal: meeting in person is a crucial factor in any trusting working relationship.

No amount of communication via email, telephone or video conferencing can permanently replace face-to-face conversation. For this very reason, we now have a highly competent contact "on the ground" in the form of Bundesbank representative Elisabetta Fiorentino.

Ms Fiorentino's professional career is a unique reflection of the close relationship shared by Germany and Italy. Having completed a joint degree programme in German and Italian, she had early experience of working in close cooperation with staff of the Banca d'Italia during her doctoral studies. Her time at the Bundesbank began in the Research Centre.

In 2009, she transitioned to the private sector, working at a large Italian bank in Milan before returning to the Bundesbank in 2013. There, her responsibilities have most recently lain in the area of financial stability.

Extended secondments to the Banque de France and the Banca d'Italia here in Rome equipped her with additional international experience. She is thus ideally primed for her new role – and as a native Italian, she should be on familiar ground.

3 Conclusion

Ladies and gentlemen,

Once Johann Wolfgang von Goethe reached Rome in 1796, he remained in the city for over three months. He then travelled on towards Sicily before returning to Rome and spending a few more months there. Unfortunately, I do not have the luxury of such an extended stay in this exquisite city. Indeed, my current "Italian journey" will come to an end in a matter of hours.

Ms Fiorentino, you will be staying in Rome for some time, making contacts, establishing relationships and fostering German-Italian cooperation. I'd like to wish you a great start and all the best in the performance of your new tasks. And to all those present, thank you very much for your attention!

Number 9

EIOPA publishes annual occupational pensions statistics

The European Insurance and Occupational Pensions Authority (EIOPA) published for the first time annual occupational pensions statistics for the reference year 2020.

The annual statistics include statistics on balance sheet, asset exposures, contributions, benefits & transfers, expenses, members and basic information, including for example information on the structure of IORPs, number of schemes and concentration ratios.

In addition to annual statistics, EIOPA already publishes quarterly statistics on basic information, balance sheet and asset exposures.

About occupational pensions statistics

The statistics contain up-to-date and high-quality data and provide a comprehensive picture of the European occupational pensions sector.

The annual statistics are derived from annual submissions to the pensions data reporting framework.

Occupational pension institutions in the EU and the European Economic Area provide the reports to their national competent authorities which EIOPA aggregates to create the statistics.

To read more:
https://www.eiopa.europa.eu/tools-and-data/occupational-pensions-statistics_en

EIOPA Occupational Pensions Statistics, Frequently Asked Questions

1. What are the EIOPA Occupational Pensions Statistics?

The publication of aggregated Occupational Pensions Statistics supports EIOPA's key strategic objectives in fostering the protection of policyholders as well as its contribution to ensure the orderly functioning of the financial system.

EIOPA's Occupational Pensions Statistics are based on Pensions Data reports from IORPs in the European Union and the European Economic Area (EEA).

These statistics provide the most up-to-date and comprehensive picture of the European Pensions sector, including country breakdowns and distributions of key variables, allowing for the comparability of high-quality data.

2. Which Institutions for occupational pension provision are included in EIOPA's Occupational Pensions Statistics?

The reported information covers institutions for occupational retirement provision (IORP) and the occupational retirement provision business of life insurance undertakings in case of Article 4 of Directive (EU) 2016/2341.

In general, the tables refer to data as of the calendar year. Where IORPs have a non-standard financial year-end, the annual statistics may not yet include all non-standard financial year-end IORPs at the publication date - these will be included in the publication in due course.

3. How often are EIOPA Occupational Pensions Statistics updated?

The statistics are published on a quarterly and an annual basis.

To read more:
https://register.eiopa.europa.eu/Publications/Pensions%20Statistics/FAQ_IORP_statistics.pdf

Number 10

NIST Seeks Public Input on Consumer Software Labeling for Cybersecurity

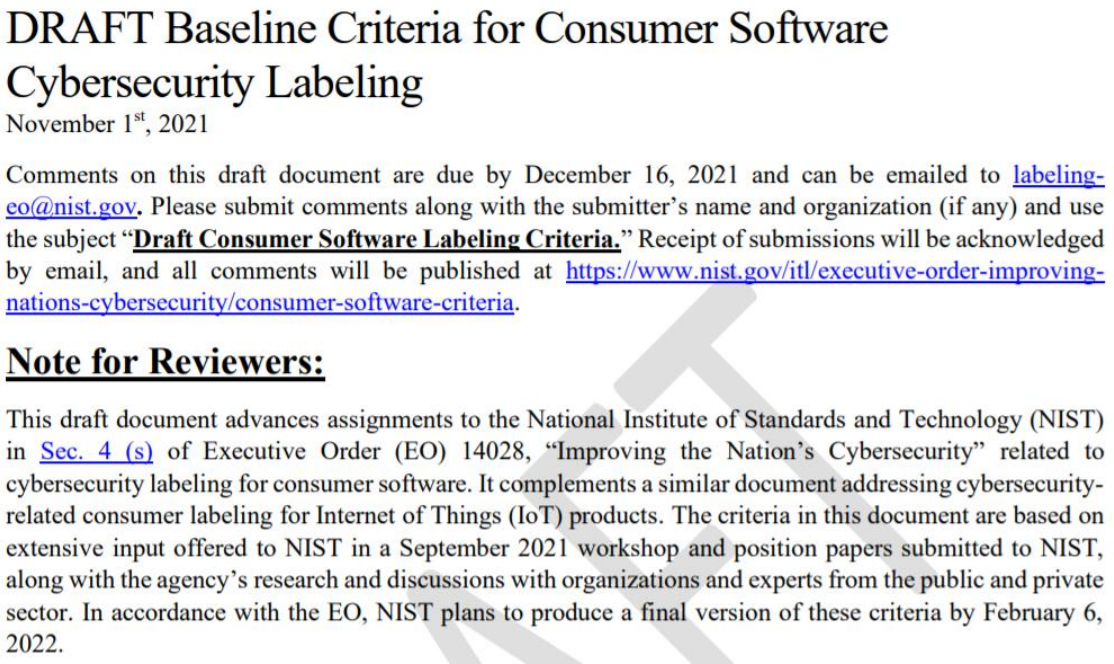
NIST is proposing key attributes of a labeling program rather than establishing its own.

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

In an effort to improve consumers' ability to make informed decisions about software they purchase, the National Institute of Standards and Technology (NIST) has drafted a set of cybersecurity criteria for consumer software. The criteria are intended to aid in the development and voluntary use of labels to indicate that the software incorporates a baseline level of security measures.

The document, formally titled *Draft Baseline Criteria for Consumer Software Cybersecurity Labeling*, forms part of NIST's response to the May 12, 2021, *Executive Order (EO) 14028 on Improving the Nation's Cybersecurity*. You may visit:
https://www.nist.gov/system/files/documents/2021/11/01/Draft%20Consumer%20Software%20Labeling.pdf

https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity



DRAFT Baseline Criteria for Consumer Software Cybersecurity Labeling

November 1st, 2021

Comments on this draft document are due by December 16, 2021 and can be emailed to labeling-eo@nist.gov. Please submit comments along with the submitter's name and organization (if any) and use the subject "**Draft Consumer Software Labeling Criteria.**" Receipt of submissions will be acknowledged by email, and all comments will be published at https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/consumer-software-criteria.

Note for Reviewers:

This draft document advances assignments to the National Institute of Standards and Technology (NIST) in Sec. 4 (s) of Executive Order (EO) 14028, "Improving the Nation's Cybersecurity" related to cybersecurity labeling for consumer software. It complements a similar document addressing cybersecurity-related consumer labeling for Internet of Things (IoT) products. The criteria in this document are based on extensive input offered to NIST in a September 2021 workshop and position papers submitted to NIST, along with the agency's research and discussions with organizations and experts from the public and private sector. In accordance with the EO, NIST plans to produce a final version of these criteria by February 6, 2022.

Federal Register
Vol. 86, No. 93
Monday, May 17, 2021

Presidential Documents

Title 3—

The President

Executive Order 14028 of May 12, 2021

Improving the Nation's Cybersecurity

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

Section 1. *Policy*. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

The EO specifies that NIST "shall identify secure software development practices or criteria for a consumer software labeling program" — criteria that reflect a baseline level of cybersecurity and that focus on ease of use for consumers. (The EO also instructs NIST to initiate a labeling effort on the cybersecurity aspects of consumer devices associated with the Internet of Things, which the present publication does not address.)

The criteria are based on suggestions from the public via position papers, a workshop, and multiple discussions with interested stakeholders. NIST is seeking public comments on the draft document by Dec. 16, 2021, to inform a final version that NIST will release on or before Feb. 6, 2022 — the deadline set in the EO. This draft is the only version that NIST plans to release before the final publication.

"We are establishing criteria for a label that will be helpful to consumers," said Michael Ogata, a NIST computer scientist and co-author of the draft document. "The goal is to raise consumers' awareness about the various security needs they might have and to help them make informed choices about the software they purchase and use."

Part of the challenge is the sheer vastness and variety of the consumer software landscape. Software forms an integral part of most consumers' lives, and it is subject to vulnerabilities that place the users' safety, property and productivity at risk — but there is no one-size-fits-all approach to cybersecurity that can be applied to all types of consumer software. The cybersecurity considerations for a smartphone game could differ greatly

from, for example, those applied to a banking app. Yet a security label aimed at consumers will need to communicate simply and directly.

While NIST's assignment is straightforward — to establish the criteria that should be the basis for a software label — NIST is not designing the label itself, nor is NIST establishing its own labeling program for consumer software. The EO calls for a voluntary approach, and it will be up to the marketplace to determine which organizations might use cybersecurity labels.

Currently, the agency is seeking public input about the baseline of technical requirements for the software and the related label. As proposed by NIST, in order to qualify for a label, the software provider would first need to meet all of the technical requirements. The document refers to these requirements as "attestations," or claims about the software's security, which the document organizes into four categories:

- Descriptive attestations — information about the label itself, such as who is making the claims about information within the label, what the label applies to and how the consumer can get more information.

- Secure software development attestations — how the software developer adheres to security best practices. By fulfilling requirements in this category, the provider communicates to consumers that they can be more confident about the development process.

- Critical cybersecurity attributes and capability attestations — features expressed by the software's functionality, and other attributes that consumers should know, such as whether the software is free from known vulnerabilities or whether encryption is used.

- Data inventory and protection attestations — information about data that consumers may identify as having high cybersecurity-related risk, and the software provider's descriptions of mechanisms used to protect that data. This data might relate to personally identifiable information, device location information, or any other data the provider has spent time and effort safeguarding.

A software label would not necessarily spell out all of these details, Ogata said, but the overall labeling effort should aim to educate consumers about what the label means and indicate where they can readily get additional information about those cybersecurity attributes. NIST is not itself planning to launch an associated education program, though software providers and others might.

“As a complement to the labeling approach, a robust consumer education program should be developed to increase label recognition and to provide transparency,” Ogata said. “Consumers should have access to online information including what the label means and does not mean, so that they can avoid potential misinterpretations. They also should know what cybersecurity properties are included in the baseline, and why and how these were selected.”

Comments on the draft document are due by Dec. 16, 2021, and can be emailed to labeling-eo@nist.gov. Please submit comments along with the submitter’s name and organization (if any) and use the subject “Draft Consumer Software Labeling Criteria." Receipt of submissions will be acknowledged by email, and all comments will be published on the project's website at: https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/consumer-software-criteria

Disclaimer

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

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

This information:

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

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

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

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

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

- is in no way constitutive of an interpretative document;

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

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

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

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

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

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

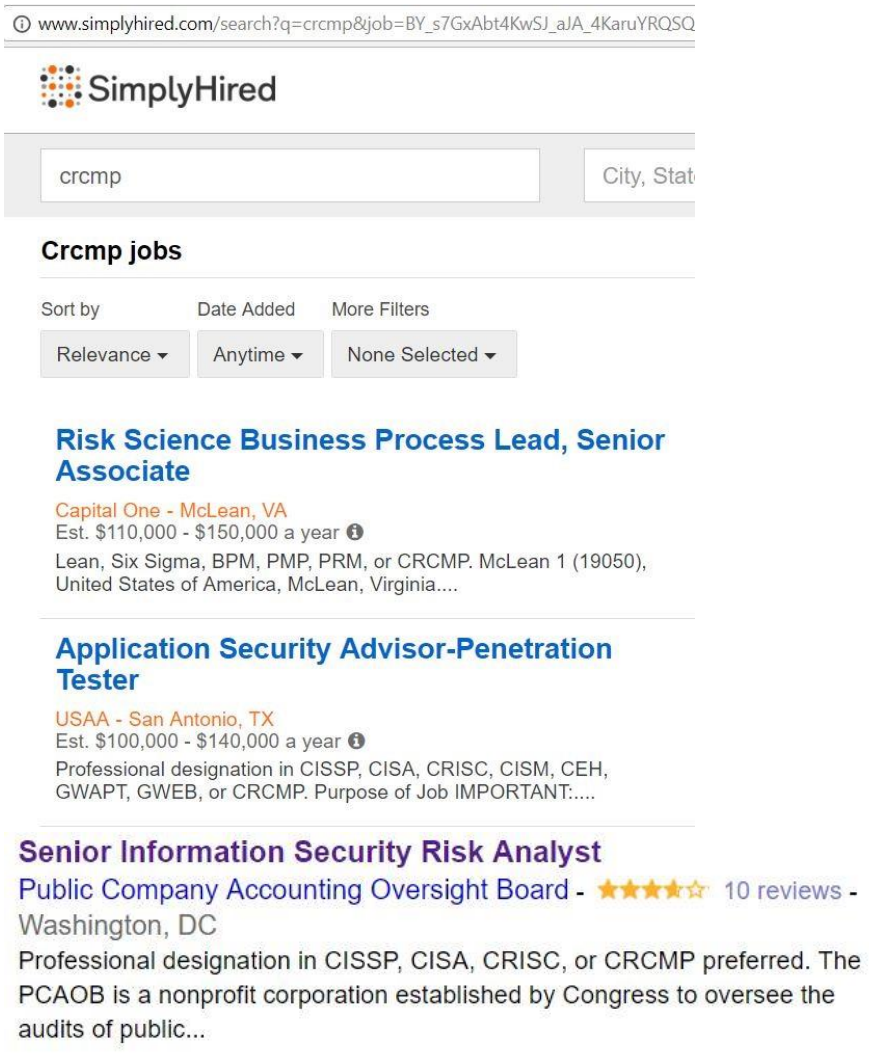
International Association of Risk and Compliance Professionals

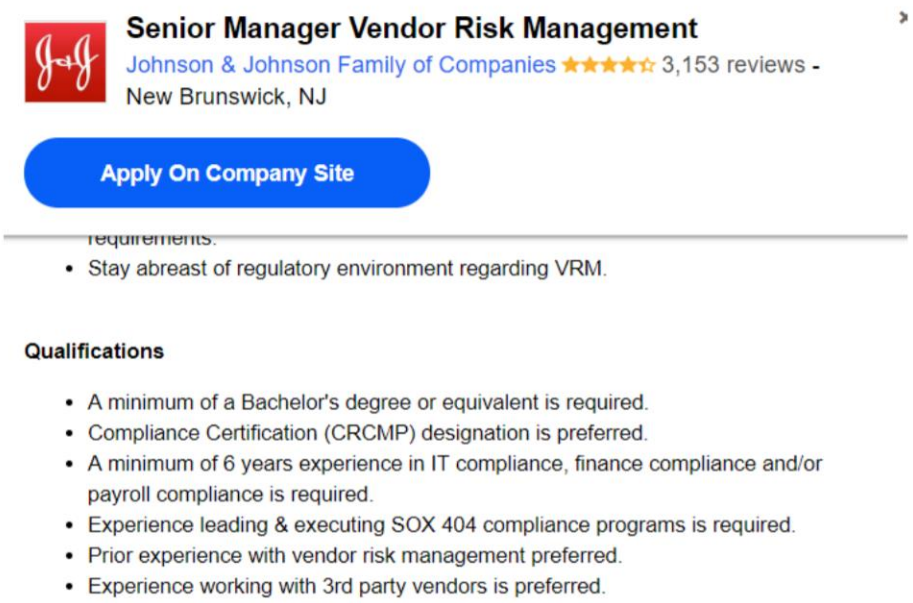
You can explore what we offer to our members:

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

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

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





Senior Manager Vendor Risk Management

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

Apply On Company Site

requirements.

- Stay abreast of regulatory environment regarding VRM.

Qualifications

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

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

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

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

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

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

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

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