International Association of Hedge Funds Professionals (IAHFP)
1200 G Street NW Suite 800 Washington DC 20005-6705 USA
Tel: 202-449-9750 Web: www.hedge-funds-association.com

Hedge Funds News, November 2021

Dear members and friends,

The Financial Stability Board (FSB) is the international body That coordinates national financial authorities and international standard-setting bodies as they work toward developing strong regulatory, supervisory and other financial sector policies. It fosters a level playing field by encouraging coherent implementation of these policies across sectors and jurisdictions. Today we will start with a very important letter:

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

This letter from the FSB Chair, Randal K. Quarles, to G20 Finance Ministers and Central Bank Governors ahead of their meeting on 13 October focuses on two key areas of the FSB's work on which the FSB has submitted reports to the upcoming G20 meeting:

Developing a more resilient NBFI sector

The letter notes that, following the market turmoil in March 2020, the FSB agreed on an ambitious multi-year workplan to enhance NBFI resilience.

A key priority of this workplan has been work to address vulnerabilities in money market funds (MMFs), conducted in collaboration with the International Organization of Securities Commission (IOSCO). The FSB has delivered to the G20 a final report with policy proposals to enhance money market fund resilience.

Table of Contents

You may visit: https://www.fsb.org/2021/10/policy-proposals-to-enhance-money-market-fund-resilience-final-report/

FSB members are assessing, or will assess, MMF vulnerabilities in their jurisdiction and will address them using the framework and policy toolkit in the report, in line with their domestic legal frameworks.

The FSB, working with IOSCO, will then take stock of progress made and assess the effectiveness of the measures taken. The FSB and IOSCO will also carry out further work, complementing MMF policy reforms, to enhance the functioning and resilience of short-term funding markets.

The letter also notes the considerable progress made on assessing vulnerabilities and identifying policy considerations in other areas within NBFI, including open-ended funds; the impact of margin calls; and the structure of core funding markets.

The FSB will leverage insights from the analysis in these areas to develop a systemic risk perspective on NBFI and policies to address such risks. The FSB will submit to G20 Leaders later this month a full progress report on its work to enhance resilience of NBFI, including areas where continued focus is needed.

Addressing challenges in cross-border payments

The COVID Event has brought into even sharper focus the need to address the limitations of current arrangements for cross-border payments.

Last year, the FSB delivered a roadmap to enhance cross-border payments, so they are faster, more inclusive, less expensive and more transparent.

Taking forward work on the roadmap, the FSB is submitting to the G20:

- a progress report on the roadmap to enhance cross-border payments, which also confirms steps for next year and beyond;

- quantitative targets for addressing the challenges of cost, speed, transparency and access experienced by end-users; and

- a report on the progress made on the implementation of the FSB's high-level recommendation for the regulation, supervision and oversight of "global stablecoin" arrangements.

The letter notes that the FSB will also be submitting its latest work on cyber incident reporting, which brings together cross-sectoral expertise to explore whether harmonisation in cyber reporting can be achieved and what additional work needs to be undertaken.

To read more: https://www.fsb.org/wp-content/uploads/P111021-1.pdf

Forum for Auditors of Small Businesses and Broker-Dealers

PCAOB Acting Chairperson Duane M. DesParte; PCAOB Staff;
FINRA Staff Event: Small Business and Broker-Dealer Auditor Forum

In September 2021, the PCAOB announced that its Forum for Auditors of Small Businesses and Broker-Dealers would not take place in person in 2021 due to the COVID-19 pandemic.

The following resources are offered in place of the in-person Forum.

Video: https://www.youtube.com/watch?v=QoxNj8ZOOuY

Video: https://www.youtube.com/watch?v=y1-PLGDV46A

The slides: https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/news/events/documents/10202021--forum-for-auditors-of-small-businesses-and-broker-dealers/final--2021-oca-presentation.pdf?sfvrsn=f56e0e0_3

Video: https://www.youtube.com/watch?v=K_CDsNSFhgM

The slides: https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/news/events/documents/10202021--forum-for-auditors-of-small-businesses-and-broker-dealers/final--2021-dei-presentation.pdf?sfvrsn=c49aa5db_3

Video: https://www.youtube.com/watch?v=JohieGTAdMk

The slides: https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/news/events/documents/10202021--forum-for-auditors-of-small-businesses-and-broker-dealers/final--dri-(issuer)-update.pdf?sfvrsn=736ea1ca_3

Video: https://www.youtube.com/watch?v=oX7P3hSmW1k

The slides: https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/news/events/documents/10202021--forum-for-auditors-of-small-businesses-and-broker-dealers/final--2021-dri-(issuer)-illustrative-examples.pdf?sfvrsn=5c7f41e6_4

To read more: https://pcaobus.org/news-events/events/event-details/2021-forum-for-auditors-of-small-businesses-and-broker-dealers

Driving different decisions today: putting climate scenarios into action

Sarah Breeden, at the MIT Golub Center for Finance and Policy 8th Annual Conference

Sarah Breeden speaks about the system-wide and economy-wide impacts of climate change, using insights from the most recent work we have led through the central banks and supervisors Network for Greening the Financial System (NGFS) on climate scenarios.

She shares lessons we have learned from designing and applying climate scenarios, as well as some thoughts on their future, including the vital contribution research needs to make.

Introduction

We are now only 11 days away from COP26 in Glasgow.

Climate science tells us that the planet has already warmed by about 1.1 degree Celsius since pre-industrial times.

Indeed, the news is full of the devastating effects of physical changes already taking place around us. And existing commitments from countries to reduce greenhouse gas emissions are not enough to keep warming to well below 2 degrees, let alone 1.5.

The United Nations Intergovernmental Panel on Climate Change (IPCC) estimates we will reach 1.5 degrees by 2040 even under their 'very low emissions' scenario.

Failure to formulate more ambitious commitments and deliver against them this decade will mean we miss the last opportunity significantly to deter the course of climate change.

The case for action is clear - the question is whether our actions will match that case, in particular whether we turn aspiration into action on the scale required. Delivering a path to net zero requires all of us to take necessary steps – governments and business, investors and individuals, as well as central banks and financial regulators.

Here at the Bank of England, we have taken a range of actions in line with our objectives – including setting expectations for banks and insurance

companies on their approaches to managing climate-related financial risks, running a system wide climate scenario exercise, and setting out how to green our corporate bond purchase scheme – to play our part in the transition to a net zero economy.

Through all this work, one thing has become abundantly clear – that the actions we take today will determine the consequences we face in the years to come. And so if we are to take the right decisions, we must stretch our horizons, taking different decisions today well before the consequences of inaction manifest at scale.

This needs to occur across the entire economy. And the financial system needs to be a key enabler. As central bank and financial regulator, these implications put climate change squarely within our remit.

We cannot solve climate change and drive the transition – those with the responsibility and tools to do this sit elsewhere in government and industry. But we must ensure that the financial system is resilient to climate-related financial risks, that it can support the transition, and that we understand its macroeconomic impacts.

Today, I want to speak specifically on the system-wide and economy-wide impacts of climate change, using insights from the most recent work we have done on climate scenarios through the central banks and supervisors Network for Greening the Financial System (NGFS).

I will cover three things: first, lessons we've learned from designing climate scenarios; second, lessons we've learned from applying them; and third, I will share some thoughts on the future of scenario analysis – including the vital contribution research needs to make.

To read more:
https://www.bankofengland.co.uk/speech/2021/october/sarah-breeden-keynote-presentation-at-the-mit

The Lack of New Bank Formations is a Significant Issue for the Banking Industry

Governor Michelle W. Bowman, at the 2021 Community Bankers Symposium: Banking on the Future, Federal Reserve Bank of Chicago, Chicago, Illinois

Good morning. I appreciate the opportunity to be part of this symposium on "Banking on the Future," especially since the future of banking is one of the highest priorities in my work at the Board.

Today, I will focus my remarks on the importance of community banks to our financial system and the challenges they face. In particular, I will focus on the formation of new banks and pose two key questions concerning the recent scarcity of these "de novo" banks.

The first question: Why have there been so few de novo bank formations over the last decade? And second, what can be done to encourage more de novo banks? I will begin with some background on community banks and bank formations.

The Importance of Community Banks

By serving communities, households, and businesses that may be underserved by larger institutions, community banks play a key role in advancing diversification in the U.S. banking system.

First and foremost, community banks provide critical financial services to their communities and to many customers who might have limited geographic access to banking services.

Because community bankers are active participants and leaders in their communities, they typically know their customers and their needs better than a banker at a branch of a larger institution.

Community banks draw upon this knowledge and conduct "relationship" lending versus relying on automated underwriting models that are typical in larger institutions.

Therefore, community banks are more willing to underwrite loans to creditworthy customers based on an assessment of qualitative factors that automated models do not consider.

Since community bankers are part of the fabric of their communities, they better understand the local market and economic conditions in the area compared to larger institutions that are not resident within the community.

Collectively, community banks are critical in advancing the health and stability of the U.S. economy as evidenced by their participation in the Small Business Administration's Paycheck Protection Program (PPP). Community banks made 4.7 million PPP loans, totaling $429 billion, which accounted for nearly 60 percent of the program's total loan amount.

In comparison with the banking industry as a whole, these banks provided more loans to traditionally underserved communities and population segments: community banks provided 87 percent of total PPP loans to minority-owned businesses, 81 percent to women-owned businesses, and 69 percent to veteran-owned businesses.

Trends in Community Banking

Despite the local and national significance of community banks, their numbers, as well as the number of insured banks in general, have been declining for several years.

This erosion of community bank charters is not just an issue in our rural communities. In urban areas, these banks, including minority-owned banks, serve businesses and households that may also be overlooked by larger institutions.

I am concerned that the contraction of community banks could lead to an unhealthy level of similarity in the banking system. As a result, this could limit the ability of households and small businesses to access credit and other types of financial products and services.

The beauty of community banks is in their differences—whether in their personality or business model. Each is unique in its mission, service delivery, and profile.

While I am troubled by the declining community bank footprint, I am not surprised that banks are choosing to merge or to be acquired. I am well aware of the significant challenges that smaller banks face. Since joining the Board, and increasingly over the past year, I have met with many state member bank CEOs who share these challenges with me.

These CEOs have expressed frustrations with ever-increasing compliance burden, which distracts their attention from prudent revenue generating activities.

As I discussed in recent remarks at the community bank research conference in late September, public policymakers must avoid adding regulatory burden on the smallest banks, particularly on those that maintain a more traditional business model.

Therefore, policymakers need to achieve a meaningful balance in our supervisory approach for community banks. Otherwise, community banks will continue to face a regulatory and supervisory framework that is ill-suited for a lower-risk profile and activities that are less complex than those of larger institutions.

Why Have There Been So Few De Novo Bank Formations over the Last Decade?

The underlying question remains: why have there been so few de novo bank formations over the last decade?

There have been only a handful of new bank charter applications over the past decade. In fact, only 44 de novo banks have been established, which include both state and national charters. A 2014 study by Federal Reserve Board economists noted that from 1990 to 2008, over 2,000 new banks were formed, which on average is more than 100 per year.

In contrast, the study noted that only seven new banks were formed from 2009 to 2013. The 2014 Board study suggests that "low interest rates and depressed demand for banking services—both of which depress profit for banks, and particularly new banks—may also have discouraged entry."

The conclusions from a Federal Reserve Bank of Kansas City study completed this year align with observations from the 2014 Board study. In this more recent study, the authors noted that new bank formations tend to be cyclical, accelerating during periods of economic expansion and slowing during recessions.

While regulatory burden has also contributed to depressed de novo formations, the authors pointed to the weak economy following the 2007-2009 financial crisis and low profitability for banking as overriding factors.

A recurring theme that has surfaced through my discussions with bankers and other industry stakeholders is the regulatory burden imposed upon de novo banks. In particular, community bankers noted the challenges in raising the capital required to establish a new bank.

The 2014 Board study noted that the states' statutory capital requirements for a new state-chartered bank could be as low as $10 million, but in practice could be as high as $30 million.

Given the high initial capital requirement, a de novo bank has a small margin of error in implementing its business strategy and meeting profit projections.

In establishing a new bank, bank executives explained the challenges in developing a business plan and risk-management framework that addresses how the bank can generate a sufficient profit to provide an adequate return to shareholders.

For a de novo bank, the cost and burden of starting from ground zero in establishing their risk-management and internal controls are high. De novo banks make strategic decisions in establishing risk-management processes and controls that may delay the launch of revenue-generating products and services.

Further, a de novo bank faces the pressure to grow quickly, which in turn, may lead to riskier lending and other activities. Indeed, experience has shown that pronounced problems often surface in the early years of a de novo bank's operations, which explains the elevated capital and supervisory expectations for these banks.

The Federal Reserve and the other banking agencies generally expect a de novo bank to maintain a Tier 1 leverage ratio of at least 8 percent for the first three years of its existence and they examine the bank on a more frequent schedule.

For a de novo bank, there is a heightened need to hire experienced staff who are quickly able to establish the bank and show progress in meeting the operating goals and profit projections in the business plan.

As we all know, difficulty in finding skilled workers is an issue more broadly in the economy, but community bankers frequently tell me of their ongoing challenges in attracting and retaining experienced staff.

These challenges are even more acute for de novo banks who require staff with experience in regulatory compliance and internal controls.

A Kansas City Reserve Banks study echoes these anecdotes, which indicate that the volume and complexity of regulations require specialized expertise that can be costly and difficult to find.

The competitive landscape for financial services and products is also a key consideration in developing and executing a de novo bank's business plan. I often hear the perspective from bankers that non-regulated financial entities have a competitive advantage over regulated financial institutions in providing financial services and products.

It would be helpful to appropriately acknowledge this competitive disadvantage for banks and tailor the regulatory framework based on the risks and complexity of their activities.

As a result, the economic, regulatory, and market realities discourage the formation of de novo banks, as investors have many other options for entry into the financial services market.

For example, they may choose to acquire an existing bank charter and subsequently establish branches in new markets. Further, they can acquire a branch office from an existing bank. And finally, they may choose to establish or acquire a nonbank financial firm that is subject to less regulation than a chartered and insured financial institution.

What Can Be Done to Encourage More De Novo Banks?

So, let's address the second question: what can be done to encourage more de novo banks?

Simply the fact that I am speaking about this topic today should give you the sense that I am concerned about the impact of the declining number of community banks. While the loss of a single community bank may be inconsequential to U.S. financial stability, that loss may have profound consequences to households and businesses in that community.

This is particularly true in rural communities and remote areas and in certain urban areas when the loss of the local bank may leave customers in a banking desert, void of tangible, relationship-based financial services.

But we should also be concerned about how a continued decline in the number of community banks, in part due to the lack of de novo formations, will affect the banking and financial services system more broadly. When banking services are limited, it is much more difficult for people to fully participate in the economy, or to manage their finances when times are tough. A shrinking community bank sector may lead to a weaker banking system and weaker economy.

It is crucial to provide a balanced, transparent, and effective regulatory framework that promotes a vibrant community bank sector.

Public policymakers need to ensure that the regulatory and supervisory framework promotes safety and soundness, while recognizing the reduced risk of these banks' noncomplex services and activities.

As large institutions and nonregulated financial companies expand their reach into markets traditionally served by community banks, policymakers

need to ensure that the regulatory and supervisory framework does not exacerbate this competitive disadvantage.

If we are not able to achieve an appropriate balance, I am concerned that there will continue to be fewer de novo banks as well as a decline in the overall population of community banks.

These banks are a key segment of the industry in that they provide financial services and products to a wide range of consumers and businesses.

Looking to the future, policymakers need to appropriately refine the regulatory and supervisory framework to minimize unnecessary compliance costs for smaller banks and address impediments to bank formations.

Closing

In conclusion, I have raised two important questions about why there so few de novo banks and what can be done to encourage new bank formations.

It is important for us to fully understand why we have seen the steady decline in bank formations, and to continue to explore ways to encourage community banks in such a competitive environment.

Identifying answers to these questions should enable the federal banking agencies to identify potential regulatory and policy constraints on the formation of new banks.

To further this effort, I have asked Federal Reserve staff to continue to study trends in community banking so that we can fully understand the economic and regulatory factors that constrain the ability of community banks to form, compete, and thrive.

I appreciate the opportunity to raise these questions with you. And I look forward to further discussions about tailoring our regulatory and supervisory framework to ensure that community banks remain an essential part of the future of the U.S. financial system.

Financial Stability Report, November 2021

This report presents the Federal Reserve Board's current assessment of the resilience of the U.S. financial system. By publishing this report, the Board intends to promote public understanding and increase transparency and accountability for the Federal Reserve's views on this topic.

Promoting financial stability is a key element in meeting the Federal Reserve's dual mandate for monetary policy regarding full employment and stable prices.

In an unstable financial system, adverse events are more likely to result in severe financial stress and disrupt the flow of credit, leading to high unemployment and great financial hardship.

Monitoring and assessing financial stability also support the Federal Reserve's regulatory and supervisory activities, which promote the safety and soundness of our nation's banks and other important financial institutions.

Information gathered while monitoring the stability of the financial system helps the Federal Reserve develop its view of the salient risks to be included in the scenarios of the stress tests and its setting of the countercyclical capital buffer (CCyB).

The Board's Financial Stability Report is similar to those published by other central banks and complements the annual report of the Financial Stability Oversight Council (FSOC), which is chaired by the Secretary of the Treasury and includes the Federal Reserve Board Chair and other financial regulators.

Framework

A stable financial system, when hit by adverse events, or "shocks," continues to meet the demands of households and businesses for financial services, such as credit provision and payment services. By contrast, in an unstable system, these same shocks are likely to have much larger effects, disrupting the flow of credit and leading to declines in employment and economic activity.

Consistent with this view of financial stability, the Federal Reserve Board's monitoring framework distinguishes between shocks to and vulnerabilities of the financial system.

Shocks, such as sudden changes to financial or economic conditions, are typically surprises and are inherently difficult to predict.

Vulnerabilities tend to build up over time and are the aspects of the financial system that are most expected to cause widespread problems in times of stress.

As a result, the framework focuses primarily on monitoring vulnerabilities and emphasizes four broad categories based on research.

1. Elevated **valuation pressures** are signaled by asset prices that are high relative to economic fundamentals or historical norms and are often driven by an increased willingness of investors to take on risk. As such, elevated valuation pressures imply a greater possibility of outsized drops in asset prices.

2. Excessive **borrowing by businesses and households** leaves them vulnerable to distress if their incomes decline or the assets they own fall in value. In the event of such shocks, businesses and households with high debt burdens may need to cut back spending sharply, affecting the overall level of economic activity. Moreover, when businesses and households cannot make payments on their loans, financial institutions and investors incur losses.

3. Excessive **leverage within the financial sector** increases the risk that financial institutions will not have the ability to absorb even modest losses when hit by adverse shocks. In those situations, institutions will be forced to cut back lending, sell their assets, or, in extreme cases, shut down. Such responses can substantially impair credit access for households and businesses.

4. **Funding risks** expose the financial system to the possibility that investors will "run" by withdrawing their funds from a particular institution or sector. Many financial institutions raise funds from the public with a commitment to return their investors' money on short notice, but those institutions then invest much of the funds in illiquid assets that are hard to sell quickly or in assets that have a long maturity.

This liquidity and maturity transformation can create an incentive for investors to withdraw funds quickly in adverse situations.

Facing a run, financial institutions may need to sell assets quickly at "fire

sale" prices, thereby incurring substantial losses and potentially even becoming insolvent.

Historians and economists often refer to widespread investor runs as "financial panics."

These vulnerabilities often interact with each other. For example, elevated valuation pressures tend to be associated with excessive borrowing by businesses and households because both borrowers and lenders are more willing to accept higher degrees of risk and leverage when asset prices are appreciating rapidly.

The associated debt and leverage, in turn, make the risk of outsized declines in asset prices more likely and more damaging. Similarly, the risk of a run on a financial institution and the consequent fire sales of assets are greatly amplified when significant leverage is involved.

It is important to note that liquidity and maturity transformation and lending to households, businesses, and financial firms are key aspects of how the financial system supports the economy.

For example, banks provide safe, liquid assets to depositors and long-term loans to households and businesses; businesses rely on loans or bonds to fund investment projects; and households benefit from a well-functioning mortgage market when buying a home.

The Federal Reserve's monitoring framework also tracks domestic and international developments to identify near-term risks—that is, plausible adverse developments or shocks that could stress the U.S. financial system.

The analysis of these risks focuses on assessing how such potential shocks may play out through the U.S. financial system, given our current assessment of the four areas of vulnerabilities.

While this framework provides a systematic way to assess financial stability, some potential risks do not fit neatly into it because they are novel or difficult to quantify.

In addition, some vulnerabilities are difficult to measure with currently available data, and the set of vulnerabilities may evolve over time.

Given these limitations, we continually rely on ongoing research by the Federal Reserve staff, academics, and other experts to improve our measurement of existing vulnerabilities and to keep pace with changes in the financial system that could create new forms of vulnerabilities or add to existing ones.

The report: https://www.federalreserve.gov/publications/files/financial-stability-report-20211108.pdf

Contents

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

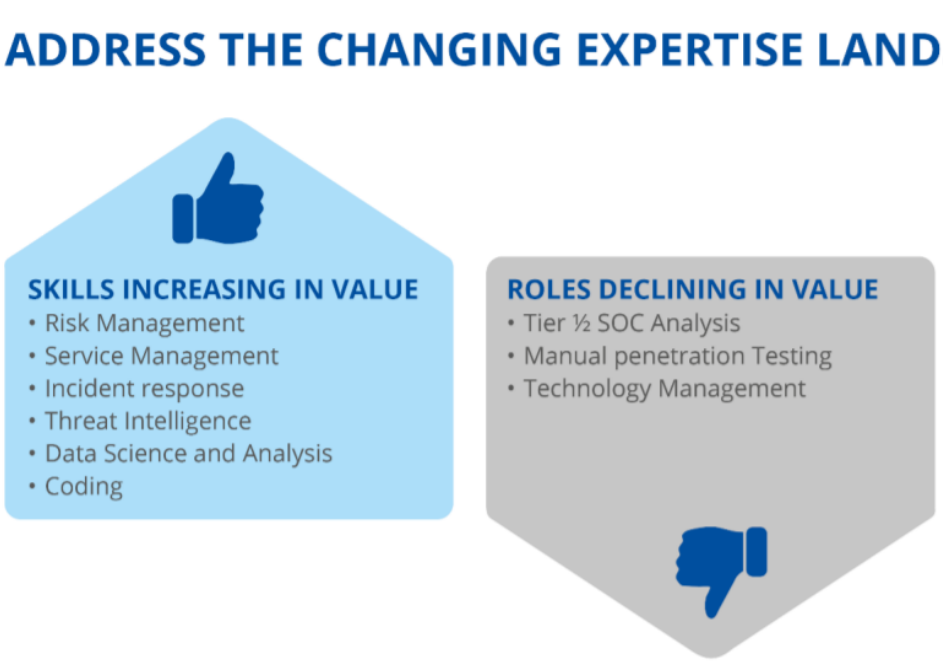
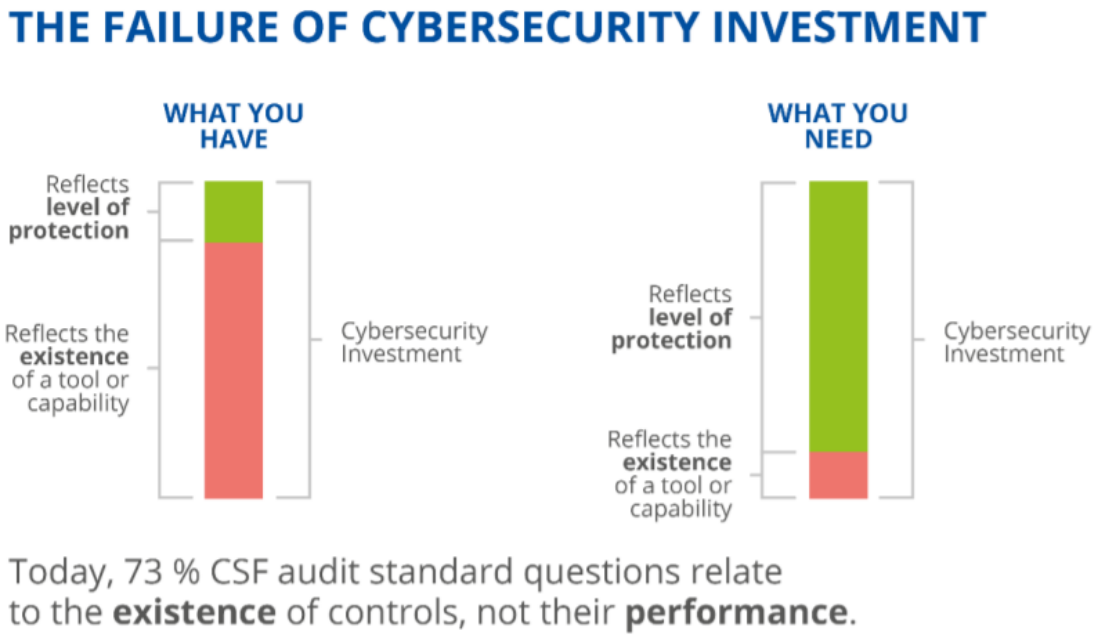


Figure 12: Cybersecurity controls – existence vs performance



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

SEC Awards $40 Million to Two Whistleblowers

U.S. SECURITIES AND EXCHANGE COMMISSION

The Securities and Exchange Commission today announced awards of approximately $40 million to two whistleblowers whose information and assistance contributed to the success of an SEC enforcement action.

The first whistleblower, whose information caused the opening of the investigation and exposed difficult-to-detect violations, will receive an award of approximately $32 million.

The first whistleblower also provided substantial assistance to the staff, including identifying witnesses and helping the staff to understand complex fact patterns.

The second whistleblower, who submitted important new information during the course of the investigation but waited several years to report to the Commission, will receive an award of approximately $8 million.

"Today's whistleblowers underscore the importance of the SEC's whistleblower program to the agency's enforcement efforts," said Emily Pasquinelli, Acting Chief of the SEC's Office of the Whistleblower. "These whistleblowers reported critical information that aided the Commission's investigation and provided extensive, ongoing cooperation that helped the Commission to stop the wrongdoing and protect the capital markets."

The SEC has awarded approximately **$1.1 billion** to 218 individuals since issuing its first award in 2012. All payments are made out of an investor protection fund established by Congress that is financed entirely through monetary sanctions paid to the SEC by securities law violators.

No money has been taken or withheld from harmed investors to pay whistleblower awards. Whistleblowers may be eligible for an award when they voluntarily provide the SEC with original, timely, and credible information that leads to a successful enforcement action.

Whistleblower awards can range from 10-30% of the money collected when the monetary sanctions exceed $1 million.

As set forth in the Dodd-Frank Act, the SEC protects the confidentiality of whistleblowers and does not disclose information that could reveal a whistleblower's identity.

For more information about the whistleblower program and how to report a tip, visit www.sec.gov/whistleblower

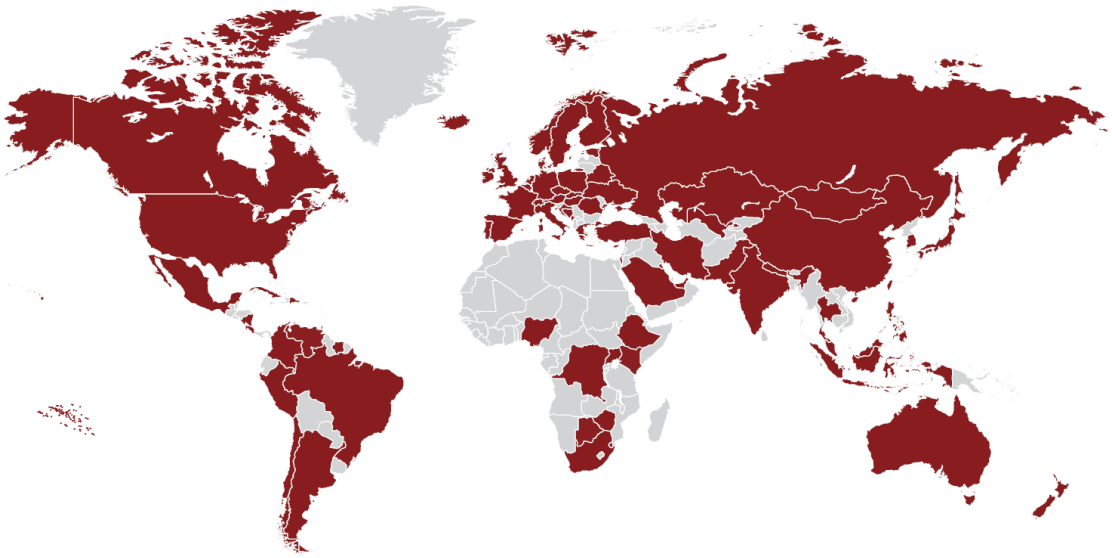
U.S. SECURITIES AND EXCHANGE COMMISSION

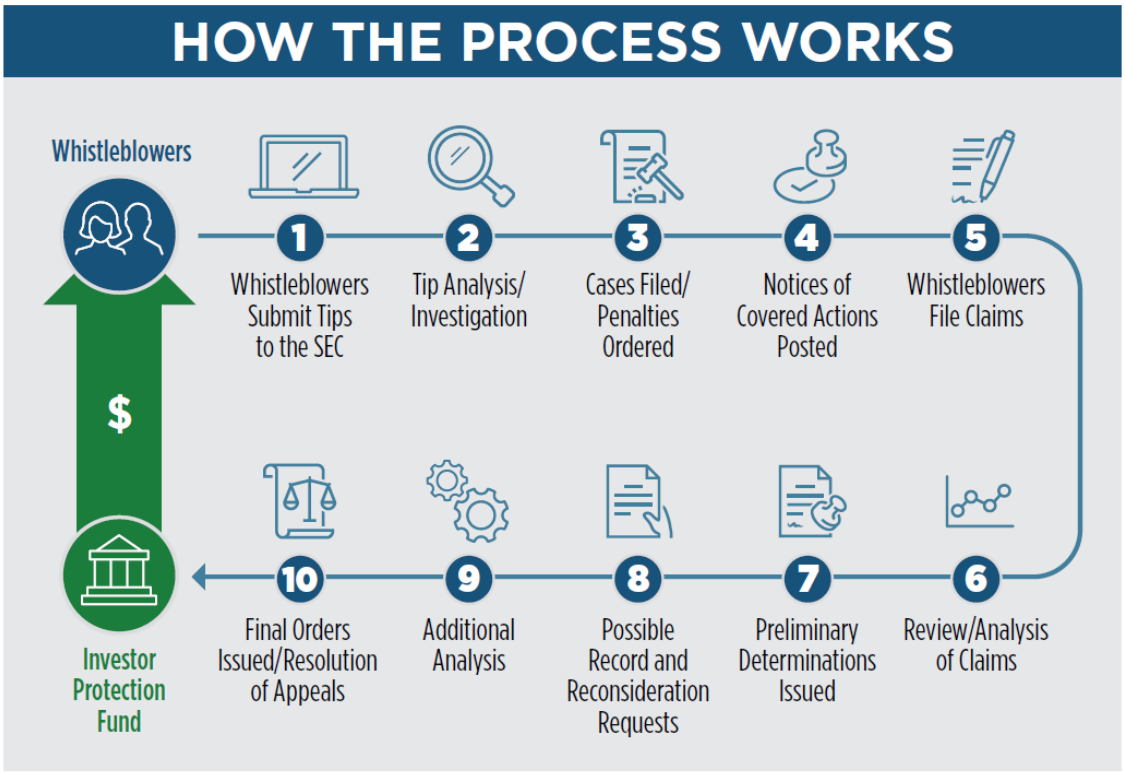
ABOUT | DIVISIONS & OFFICES | ENFORCEMENT | REGULATION

Office of the Whistleblower

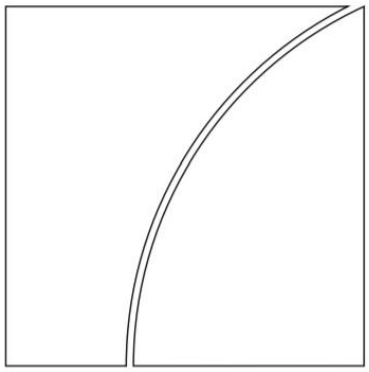
Office of the Whistleblower

The map below reflects the countries in which whistleblower tips originated during FY 2020.




HOW THE PROCESS WORKS
Whistleblowers
$
Investor Protection Fund
1
Whistleblowers Submit Tips to the SEC
2
Tip Analysis/ Investigation
3
Cases Filed/ Penalties Ordered
4
Notices of Covered Actions Posted
5
Whistleblowers File Claims
6
Review/Analysis of Claims
7
Preliminary Determinations Issued
8
Possible Record and Reconsideration Requests
9
Additional Analysis
10
Final Orders Issued/Resolution of Appeals

Big techs in finance: on the new nexus between data privacy and competition



BIS Working Papers
No 970

Big techs in finance: on the new nexus between data privacy and competition

by Frederic Boissay, Torsten Ehlers, Leonardo Gambacorta and Hyun Song Shin

Monetary and Economic Department

October 2021

Focus

Large technology companies such as Alibaba, Amazon, Facebook, Google and Tencent have started to provide financial services. The activities of big techs in finance are a special case of broader fintech innovation.

While fintech companies are set up to operate primarily in financial services, big tech firms offer financial services as part of a much wider set of activities. Big techs' foray into finance raises both opportunities and risks.

Contribution

The contribution of this paper is threefold.

First, it describes big techs' business models and analyses the potential benefits in their provision of financial services such as financial inclusion and reduced asymmetric information problems in the supply of credit.

Second, it evaluates the potential costs, including the new risks of price discrimination, abuse of market power, anti-competitive behaviour and limits to data privacy.

Third, it lays out the complex public policy trade-off between the objectives of efficiency and privacy, and discusses the policy options

Findings

Big techs' entry in finance builds on their established digital platforms in e-commerce, search and social media, and holds the prospect of efficiency gains and greater financial inclusion.

Their business model rests on enabling direct interactions among a large number of users.

An essential by-product of their business is their large stock of user data, which are used as an input for a range of services that exploit natural network effects, generating further user activity.

Increased user activity then completes the circle, as it generates yet more data.

The self-reinforcing loop between data, network externalities and activities, is the DNA of big techs.

Big techs have the potential to become dominant through the advantages afforded by the data-network-activities DNA loop – raising competition and data privacy issues.

How to define and regulate the use of data has become an important policy issue for authorities and increases the need to coordinate policies at both the domestic and international level.

Abstract

The business model of big techs rests on enabling direct interactions among a large number of users on digital platforms, such as in e-commerce, search and social media.

An essential by-product is their large stock of user data, which they use to offer a wide range of services and exploit natural network effects, generating further user activity.

Increased user activity completes the circle, as it generates yet more data.

Building on the self-reinforcing nature of the data- network-activities loop, some big techs have ventured into financial services, including payments, money management, insurance and lending.

The entry of big techs into finance promises efficiency gains and greater financial inclusion.

At the same time, it introduces new risks associated with market power and data privacy.

The nature of the new trade-off between efficiency and privacy will depend on societal preferences, and will vary across jurisdictions.

This increases the need to coordinate policies both at the domestic and international level.

You may visit: https://www.bis.org/publ/work970.pdf

Ongoing Cyber Threats to U.S. Water and Wastewater Systems

This joint advisory is the result of analytic efforts between the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Agency (CISA), the Environmental Protection Agency (EPA), and the National Security Agency (NSA) to highlight ongoing malicious cyber activity—by both known and unknown actors—targeting the information technology (IT) and operational technology (OT) networks, systems, and devices of U.S. Water and Wastewater Systems (WWS) Sector facilities. You may visit: https://www.cisa.gov/water-and-wastewater-systems-sector

This activity—which includes attempts to compromise system integrity via unauthorized access—threatens the ability of WWS facilities to provide clean, potable water to, and effectively manage the wastewater of, their communities.

Note: although cyber threats across critical infrastructure sectors are increasing, this advisory does not intend to indicate greater targeting of the WWS Sector versus others. To secure WWS facilities—including Department of Defense (DoD) water treatment facilities in the United States and abroad—against the TTPs listed below, CISA, FBI, EPA, and NSA strongly urge organizations to implement the measures described in the Recommended Mitigations section of this advisory.

THREAT OVERVIEW
Tactics, Techniques, and Procedures

WWS facilities may be vulnerable to the following common tactics, techniques, and procedures (TTPs) used by threat actors to compromise IT and OT networks, systems, and devices.

• *Spearphishing personnel to deliver malicious payloads, including ransomware.*

o Spearphishing is one of the most prevalent techniques used for initial access to IT networks. Personnel and their potential lack of cyber awareness are a vulnerability within an organization. Personnel may open malicious attachments or links to execute malicious payloads contained in emails from threat actors that have successfully bypassed email filtering controls.

o When organizations integrate IT with OT systems, attackers can gain access—either purposefully or inadvertently—to OT assets after the IT

network has been compromised through spearphishing and other techniques.

o Exploitation of internet-connected services and applications that enable remote access to WWS networks.

o For example, threat actors can exploit a Remote Desktop Protocol (RDP) that is insecurely connected to the internet to infect a network with ransomware. If the RDP is used for process control equipment, the attacker could also compromise WWS operations. Note: the increased use of remote operations due to the COVID-19 pandemic has likely increased the prevalence of weaknesses associated with remote access.

• *Exploitation of unsupported or outdated operating systems and software.*

o Threat actors likely seek to take advantage of perceived weaknesses among organizations that either do not have—or choose not to prioritize—resources for IT/OT infrastructure modernization. WWS facilities tend to allocate resources to physical infrastructure in need of replacement or repair (e.g., pipes) rather than IT/OT infrastructure.

o The fact that WWS facilities are inconsistently resourced municipal systems—not all of which have the resources to employ consistently high cybersecurity standards—may contribute to the use of unsupported or outdated operating systems and software.

• *Exploitation of control system devices with vulnerable firmware versions.*

o WWS systems commonly use outdated control system devices or firmware versions, which expose WWS networks to publicly accessible and remotely executable vulnerabilities. Successful compromise of these devices may lead to loss of system control, denial of service, or loss of sensitive data.

WWS Sector Cyber Intrusions

Cyber intrusions targeting U.S. WWS facilities highlight vulnerabilities associated with the following threats:

• Insider threats from current or former employees who maintain improperly active credentials

• Ransomware attacks

WWS Sector cyber intrusions from 2019 to early 2021 include:

• In August 2021, malicious cyber actors used Ghost variant ransomware against a Californiabased WWS facility. The ransomware variant had been in the system for about a month and was discovered when three supervisory control and data acquisition (SCADA) servers displayed a ransomware message.

• In July 2021, cyber actors used remote access to introduce ZuCaNo ransomware onto a Maine-based WWS facility's wastewater SCADA computer. The treatment system was run manually until the SCADA computer was restored using local control and more frequent operator rounds.

• In March 2021, cyber actors used an unknown ransomware variant against a Nevada-based WWS facility. The ransomware affected the victim's SCADA system and backup systems. The SCADA system provides visibility and monitoring but is not a full industrial control system (ICS).

• In September 2020, personnel at a New Jersey-based WWS facility discovered potential Makop ransomware had compromised files within their system.

• In March 2019, a former employee at Kansas-based WWS facility unsuccessfully attempted to threaten drinking water safety by using his user credentials, which had not been revoked at the time of his resignation, to remotely access a facility computer.

To read more: https://us-cert.cisa.gov/sites/default/files/publications/AA21-287A-Ongoing_Cyber_Threats_to_U.S._Water_and_Wastewater_Systems.pdf

Fiscal Year 2022, Bank Supervision Operating Plan

Office of the Comptroller of the Currency, Committee on Bank Supervision

The Office of the Comptroller of the Currency's (OCC) Committee on Bank Supervision (CBS) strategy planning guidance sets forth the agency's supervision priorities and objectives.

The agency's fiscal year (FY) for 2022 begins October 1, 2021, and ends September 30, 2022.

The FY 2022 Bank Supervision Strategy Planning Guidance outlines the OCC's supervision priorities and aligns with "The OCC's Strategic Plan, Fiscal Years 2019–2023" and the National Risk Committee's (NRC) priorities.

The strategy planning guidance facilitates the development of supervisory strategies for individual national banks, federal savings associations, federal branches, and agencies of foreign banking organizations (collectively, banks), as well as identified service providers.

CBS managers and staff will use this plan to guide their supervisory priorities, planning, and resource allocations for FY 2022.

Priority Objectives for CBS Operating Units

The FY 2022 strategy planning guidance and the FY 2022 Bank Supervision Operating Plan establish priority objectives across the CBS operating units.

CBS operating units and managers should use this guidance to develop and execute individual operating unit plans and risk-focused bank supervisory strategies.

While the objectives are similar for the Large Bank Supervision and Midsize and Community Bank Supervision, CBS managers will differentiate bank size, complexity, and risk profile when developing individual bank supervisory strategies.

CBS operating plans include resources and support for risk-focused examinations of technology and significant service providers that provide critical processing and services to banks.
The OCC will adjust supervisory strategies, as appropriate, during the fiscal year in response to emerging risks and supervisory priorities.

For FY 2022, supervision will focus on the impacts of the pandemic and resulting economic, financial, operational, and compliance implications.

In addition to the baseline supervision to assign ratings, examiners will focus on the safety and soundness of strategic and operational planning, including:

• **Guarding against complacency:** Examiners should focus on strategic and operational planning to ensure banks maintain stable financial positions, especially regarding capital, the allowances for credit losses, management of net interest margins, and earnings.

Examiners should ensure banks remain vigilant when considering growth and new profit opportunities and will assess management's and the board's understanding of the impact of new activities on the bank's financial performance, strategic planning process, and risk profile.

• **Credit:** Examiners should evaluate banks' actions to manage credit risk given changes in market condition, termination of pandemic-related forbearance, uncertainties in the economy, and the lasting impacts of the COVID-19 pandemic.

Supervisory focus should ensure that risk management functions are providing an appropriate credible challenge. Examiners will evaluate underwriting practices on new or renewed loans for easing in structure and terms. Reviews will focus on new products, areas of highest growth, or portfolios that represent concentrations.

Supervisory focus should include those portfolios hard hit by the pandemic that may experience amplified impacts from changes in market conditions.

• **Allowance for loan and lease losses (ALLL)/allowance for credit losses (ACL):** For all banks, examiners should focus on ALLL and ACL adequacy considering any stress on credit portfolios.

U.S. Securities and Exchange Commission (SEC) filers, except small reporting companies as defined by the SEC, were required to adopt the current expected credit losses (CECL) accounting standard in 2020 but could delay adoption until 2022.

All other banks are required to implement CECL by 2023. For banks that have not yet adopted CECL, examiners should evaluate preparedness, including bank implementation plans and use of third parties to assist in the development of the loss estimation methodology, modeling techniques, and management information systems.

Additional impacts may include post-hardship performance of borrowers assisted with streamlined deferral and loan modifications.

For banks that have adopted CECL, examiners should evaluate the effectiveness of the methodology at estimating lifetime expected credit losses.

• **Cybersecurity:** Operational risk, resilience, incident response, and data recovery and business resumption should be supervisory focal points. Examinations should assess the bank's capabilities to recover from destructive malware attacks.

Examinations should emphasize threat vulnerability and detection, authentication and access controls, network management, data management, and managing third-party access.

Examiners should perform assessments of internal controls and operational processes that changed during the pandemic.

• **Third parties and related concentrations:** Examiners should determine whether banks are providing proper oversight of their significant third-party relationships, including partnerships.

Examiners should identify where those relationships are critical to bank operations and understand whether they represent significant concentrations or impact resiliency.

Examiners should also be aware of the cyber-related risks emanating from third parties and evaluate the bank assessments of the third party's cybersecurity risk management and resilience capabilities.

• **Bank Secrecy Act, consumer compliance, and fair lending:**

- **BSA/AML and Office of Foreign Assets Control:** Strategies should continue to focus on BSA/AML compliance, with emphasis on evaluating the effectiveness of BSA/AML risk management systems relative to the complexity of business models, products and services offered, and customers and geographies served; evaluating technology and modeling solutions to perform or enhance BSA/AML oversight functions; and determining the adequacy of suspicious activity monitoring and reporting systems and processes in providing meaningful information to law enforcement.

  Examiners should also begin to assess bank change management plans for implementing changes to existing BSA/AML compliance programs

that will be required regulatory changes to implement the Anti-Money Laundering Act of 2020.

- **Consumer compliance:** Examiners should focus on compliance management systems, including third-party risk management and higher risk products and services such as overdraft protection programs, particularly focusing on how the programs are implemented and how terms of the programs are disclosed.

  Examiners should consider the effect that earnings pressure has had on banks, monitoring the effect that may have had on the compliance risk management functions, if any, through cutting personnel or waiving audits.

- **Fair lending:** Examiners should focus on assessing fair lending risk, considering changes to the bank's products, services, and operating environments.

  These should be based upon the bank's fair lending risk profile and the annual Home Mortgage Disclosure Act data screening process. Fair lending supervision activities should consider the full lifecycle of credit products (e.g., mortgages).

- **CRA:** OCC Bulletin 2020-99, "Community Reinvestment Act: Key Provisions of the June 2020 CRA Rule and Frequently Asked Questions," provides updated guidance following issuance of the OCC's June 2020 rule.

  Examiners should be familiar with this set of policies and procedures and plan accordingly for examinations that cover calendar years before and during the time that the 2020 rule is in effect.

  In addition, the OCC has proposed to rescind the June 2020 rule and replace it with rules largely like the 1995 CRA rules. Examiners should plan on additional training on these rule changes and to incorporate new CRA policy or process guidance issued during FY2022.

• **Interest rate risk:** Examiners should assess the impact of a low-rate environment on banks' business models, strategies, asset and liability risk exposures, net interest margin, funding stability, and modeling capabilities.

• **London Interbank Offered Rate (LIBOR):** Examiners should evaluate each bank's implementation and execution of alternative reference rates given the December 30, 2021, cessation of LIBOR.

Banks should fully understand all their exposures and be nearly complete with remediation efforts. Examiners should evaluate operational, reputation, and consumer impact assessments and change management related to an alternative index for pricing loans, deposits, and other products and services.

• **Payments:** Examiners should evaluate payment systems products and services that banks offer or plan to offer, with a focus on new or novel products, services, or channels for wholesale and retail customer relationships.

Examiners should consider potential risks including operational, compliance, strategic, credit, and reputation and how these risks are incorporated into institution-wide risk assessments and new product review processes, if applicable.

• **Fintech/Cryptocurrency:** Examiners should identify banks that are implementing significant changes in their operations using new technological innovations and evaluate implementation, including use of cloud computing, artificial intelligence, and digitalization in the risk management processes.

Examiners should evaluate the appropriateness of governance processes when banks undertake significant changes.

• **Climate:** The OCC is working to better understand how the financial risks associated with climate change may affect the safety and soundness of institutions including their ability to serve all parts of their communities.

During FY2022, the agency will continue information gathering efforts and plan on conducting additional industry outreach.

At the largest banks, examiners should focus on establishing a baseline understanding of the effects of physical and transition risks including the development of climate risk management frameworks and governance processes.

Resources should focus on significant risks in FY2022 while considering appropriate coverage of other areas. Strategies should focus on control functions and leverage the institutions' audit, loan review, and risk management processes when the OCC has validated reliability.

To facilitate an agency-wide view of risk on selected topics, the CBS operating units will prioritize and coordinate resources and conduct horizontal risk assessments during the fiscal year. The CBS may direct horizontal assessments during the supervisory cycle.

The OCC will provide periodic updates about supervisory priorities, emerging risks, and horizontal risk assessments in the Semiannual Risk Perspective report.

Cyber risks: what is the impact on the insurance industry?

October is the European cyber security month. As cyber attacks are a continuing risk for insurers, in this article we are discussing their incidence in the financial industry as a whole and among insurers in particular, why insurers are on the radar and what are the consequences for insurers and for policyholders.

The pandemic has accelerated the digital transformation. Financial institutions have increased their use of information technology. They are now more heavily relying on digital and remote solutions to perform their daily operations and to deliver their services to customers.

While this has brought along benefits, the increasing reliance on digital solutions has also expanded the risk for cyber attacks.

Cyber risks are considered as a top global risk for the financial sector and the economy as a whole. The type of ICT risks to which the undertakings are exposed have not changed in the past years, however the frequency of incidents and the magnitude of their impact on financial entities has increased.

A recent study on Covid-19 and cyber risk in the financial sector revealed that the financial sector has experienced the largest number of Covid-19-related cyber events after the health sector. Payment institutions, insurers and credit unions are the most affected.

Insurers in some jurisdictions are reporting an increasing number of malware and other cyber attempts.

Insurance supervisors consider cyber security risks as the main trigger of other risks, as highlighted by the European Supervisory Authorities (EIOPA, ESMA and EBA) in their report on the risks and vulnerabilities in the financial sector.

Some of these risks include:

- digitalisation risks (for 73% of insurance supervisors)
- cyber underwriting risks (19%)
- InsurTech competition (8%)

Why insurers are on the radar of cyber attacks ?

Insurance groups are a natural target for cyber attacks because they possess substantial amounts of confidential policyholder data. Products, policies and pricing are all powered by data.

This is what makes it so valuable: with data an insurance company is able to offer the consumer just what they need and hopefully at just the right price. More choice and lower costs are what makes consumers so ready to share their data.

In contrast to other sectors, which hold mainly sensitive financial data, insurers typically also collect a large amount of protected personal sensitive information.

What are the consequences?

The main consequences suffered by insurers following these cyber incidents are business interruption and material costs for the undertaking, for policyholders and for third parties.

Data obtained can be used for different criminal purposes such as identity theft to obtain financial gains.

Besides the direct financial consequences, cyber incidents can also result in severe and long-lasting operational issues for the targeted insurance groups. The reputational damage may also be substantial or even irreversible.

If malicious cyber incidents cause business interruptions, this has a direct impact on all policyholders.

At the same time, as a direct consequence of the increase of ICT incidents as described above the cyber-underwriting market is expanding. According to Statista, the European cyber insurance market is expected to grow exponentially between 2020 and 2030, doubling in size between 2020 and 2025. Insurers have their role to play in this area. A sound cyber insurance market is an important measure. The challenge is how to insure and help prevent cyber risk.

In conclusion, insurers and pension funds need not only to manage cyber and IT risk within the company and the value chain, but they also need to keep pace with new threats and developments. Here operational resilience testing and cooperation can help and as such EIOPA welcomes the Digital Operational Resilience Act, or DORA and other initiatives in this field and stands ready to contribute.

The Digital Operational Resilience Act (DORA): https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&from=EN

Brussels, 24.9.2020
COM(2020) 595 final

2020/0266 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014

EIOPA will continue to monitor and motivate innovation, while keeping a close eye on new risks that are emerging, as well as on how consumers are served.

Progress report on adoption of the Basel regulatory framework

BIS

The Basel Committee on Banking Supervision (BCBS) and its oversight body, the Group of Central Bank Governors and Heads of Supervision (GHOS) have set as high priority the full, timely and consistent implementation of all aspects of the Basel III framework.

This includes the finalised Basel III post-crisis reforms published by the Committee in December 2017 and set to go into effect on 1 January 2023 with a five-year phase-in.

Continuing the periodic monitoring initiated a decade ago, this report sets out the adoption status of Basel III standards for each of the BCBS member jurisdictions as of end-September 2021.

It is part of the broader Committee's Regulatory Consistency Assessment Programme (RCAP) established to monitor progress in introducing corresponding domestic regulations, assessing their consistency and analysing regulatory outcomes.

Despite the disruptions resulting from Covid-19 and the required shift in regulatory and supervisory priorities, further progress has been made in the implementation of the Basel III standards especially those with deadlines that have already passed.

In fact, many jurisdictions used the existing flexibilities in the Basel framework to provide regulatory relief during the pandemic.

All jurisdictions now have final rules in force for the countercyclical capital buffer (CCyB). Overall, in respect of the outstanding capital standards there have been 11 new adoptions.

This includes three additional jurisdictions which have adopted final rules with regard to total loss-absorbing capacity (TLAC), and two additional jurisdictions which have adopted final rules with regard to the standardised approach for measuring counterparty credit risk exposure (SA-CCR) and capital requirements for equity investments in funds.

An additional four jurisdictions have adopted the Net Stable Funding Ratio (NSFR) standard. Further, across the disclosure parts of the framework there have been seven additions. In respect of the Basel III standards which have a deadline in the future, there have been new adopters of the revised operational risk framework and revised standardised approach for credit risk.

The report excludes standards that had previously been implemented by all jurisdictions such as the Liquidity Coverage Ratio (LCR) and capital conservation buffers (CCoB) and is based on Basel adoption status updates submitted by jurisdictions as of end-September 2021.

A complete view by standard and jurisdiction is provided in the Overview section followed by summary information about the implementation status and adoption plans for each of the 27 jurisdictions and the EU.

Table 1: Member jurisdictions that have issued final rules

Standard		Number of jurisdictions as of end-May 2020	Number of jurisdictions as of end-September 2021	Increase in adoption
Capital	Countercyclical capital buffer	26	27	1
	Margin requirements for non-centrally cleared derivatives	19	20	1
	Capital requirements for CCPs	21	22	1
	Capital requirements for equity investments in funds	19	21	2
	SA-CCR	23	25	2
	Securitisation framework	21	22	1
	TLAC holdings	18	20	3*
	Revised standardised approach for credit risk	1	2	1
	Revised operational risk framework	2	5	3
Liquidity	Net Stable Funding Ratio (NSFR)	22	26	4
Disclosure	CCyB, Liquidity, Remuneration, Leverage ratio (revised)	20	21	1
	Key metrics, IRRBB, NSFR	15	18	3
	Composition of capital, RWA overview, Prudential valuation adjustments, G-SIB indicators	19	20	1
	TLAC Disclosure	15	17	2

* The increase in adoption is actually three in 2021 rather than two. This is because one jurisdiction revised its TLAC status from fully adopted (4) to not applicable (na) during this period.

Table 1 highlights the progress made since the last report published in July 2020 by listing the standards with an increase in the number of jurisdictions with final rules in place.

The shaded area indicates the standards with deadlines in the future. Further evaluation of the consistency of jurisdictional implementation is addressed through the RCAP assessments. The outstanding RCAP on NSFR and large exposures framework (LEX) are expected to resume soon after they were suspended last year in response to Covid-19.

Overview of implementation

	Basel standards	Deadline	AR	AU	BR	CA	CN	HK	IN	ID	JP	KR	MX	RU	SA	SG	ZA	CH	TR	UK	US	EU
Capital	Countercyclical capital buffer	Jan 2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
	Margin requirements for non-centrally cleared derivatives	Sep 2016	1	4	4	4	1	4	2	2	4	3	2	2	4	4	4	4	1	4	4	4
	Capital requirements for CCPs	Jan 2017	4	4	4	4	1	4	3	2	4	4	1	2	4	4	4	4	2	3	3	4
	Capital requirements for equity investments in funds	Jan 2017	4	4	4	4	1	2	na	na	4	4	*	4	4	4	4	4	4	3	1	4
	SA-CCR	Jan 2017	4	4	4	4	4	4	3	4	4	4	1	4	4	4	4	4	2	3	3	4
	Securitisation framework	Jan 2018	4	4	4	4	1	4	4	4	4	4	1	4	4	4	2	4	1	4	1	4
	TLAC holdings	Jan 2019	na	4	4	4	2	4	1	na	4	1	4	4	4	4	2	4	1	4	4	4
	Revised standardised approach for credit risk	Jan 2023	1	2	2	2	1	1	1	2	2	3	4	2	1	2	1	1	1	1	1	1
	Revised IRB approach for credit risk	Jan 2023	na	2	1	2	1	1	1	na	2	3	1	4	1	2	1	1	1	1	1	1
	Revised CVA framework	Jan 2023	1	1	1	2	1	1	1	2	2	1	1	1	1	2	1	1	1	1	1	1
	Revised minimum requirements for market risk	Jan 2023	1	1	*	2	1	1	1	2	2	1	1	1	2	2	1	1	1	1	1	*
	Revised operational risk framework	Jan 2023	1	3	1	2	1	1	1	3	2	3	4	4	2	2	1	1	1	1	1	1

Status classification code (numerical code):

4=Final rule in force: the domestic legal or regulatory framework has been published and is implemented by banks;

3=Final rule published: the domestic legal or regulatory framework has been published but is not implemented by banks;

2=Draft regulation published: a draft law, regulation or other official document has been made public and is specific enough to be implemented;

1=Draft regulation not published: no draft law, regulation or other official document has been made public to detail the planned content of the domestic regulatory rules.

This status includes cases where a jurisdiction has communicated high-level information about its implementation plans, but not detailed rules.

* = Cases where the implementation status for the full standard is partial are indicated with an asterisk;

na = not applicable.

Applicable standards for which the agreed implementation deadline has passed receive a colour code to reflect the status (colour code):
green = adoption completed;
yellow = adoption in process (at least some draft regulation published);
red = adoption not started (no draft regulation published yet).

A standard is deemed to be adopted and implemented when the numerical code is 4 and the colour code is green.

To read more: https://www.bis.org/bcbs/publ/d525.pdf

BaFin amends its BAIT

In the current amendment to the BAIT, BaFin clarifies its expectations for IT and information security at banks.
Thorsten Sämisch, BaFin IT Supervision Group

BaFin Federal Financial Supervisory Authority

On 16 August 2021, BaFin published the new version of its BAIT, the Supervisory Requirements for IT in Financial Institutions. The amendment came into force on the same date.

BaFin is using this amendment to set out the overall conditions it now expects for secure information processing and information technology.

There are no transitional periods because BaFin is not imposing any fundamental new requirements, but has clarified existing requirements.

Background to the amendment

Guidelines issued by the European Banking Authority (EBA) in November 2019 form part of the backdrop to the BAIT amendment. You may visit: https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management

In its Guidelines on ICT and security risk management (EBA/GL/2019/04), the EBA had previously responded to the European Commission's FinTech action plan and introduced standardised requirements for the entire single market: for credit institutions, investment firms and payment service providers.

The EBA thus established the corresponding framework for the supervisory practice of the national competent authorities.

Together with the Deutsche Bundesbank, BaFin then examined whether, and to what extent, the BAIT would have to be supplemented and adapted. Experience gained from supervisory practice was also expected to be incorporated into the work.

The IT expert committee, whose members are representatives of the trade associations of the banking sector, smaller and larger institutions, as well as BaFin and Bundesbank staff, was also closely involved in the amendment. The Federal Ministry of Finance also participated.

A public consultation on the BAIT amendment was launched in autumn 2020.

Because the content of the BAIT builds on the Minimum Requirements for Risk Management (MaRisk) , the BAIT amendment was developed in parallel with the sixth amendment to MaRisk, and both circulars were published at the same time.

Significant amendments

Even though there were no fundamental changes, some parts of the BAIT were expanded and adapted.

In the new "Operational information security" chapter, for example, BaFin sets out requirements for the design of effectiveness controls of information security measures that have already been implemented in the shape of tests and exercises.

Such effectiveness controls, for example gap analysis, vulnerability scans, penetration tests and simulated attacks, are a key element of any effective, sustainable information security management system.

The institutions must verify the security of the IT systems regularly and on an event-driven basis. They must avoid conflicts of interest when they do so: for example, anybody involved in planning and implementing security measures cannot subsequently test them.

The institutions have to analyse the results of such effectiveness controls, identify any need for improvement and manage risks appropriately.

The institutions are expected to document the new requirements in an internal policy that BaFin now calls for in the "Information security management" chapter.

This chapter also contains requirements relating to logging and monitoring, in other words recording results and real-time monitoring, as well as the identification and analysis of security-related events.

For example, potentially security-related information must be evaluated suitably promptly, using a rule-based approach, and must be held available for an appropriate period for subsequent evaluation.

To do this, a portfolio of rules for identifying security-related events must be defined and updated.

The expanded AT 7.3 "Contingency management" in the new MaRisk forms the basis for the new BAIT chapter "IT contingency management".

It stipulates the establishment of restart, emergency operation and recovery plans for time-critical processes and activities.

According to the BAIT, the institutions must verify annually that these three types of IT contingency plan are effective – based on an IT testing concept.

The new third chapter in the BAIT is called “Managing relationships with payment service users”.

It is taken from the new circular “Supervisory Requirements for IT in Payment Services and Electronic Money Institutions” (ZAIT). Its content is also relevant for large parts of the BAIT target group.

Information security instead of IT security

It was also important for BaFin and the Deutsche Bundesbank to follow the objective of “information security” in the BAIT and not the – narrower – objective of “IT security”.

Traditional IT security is limited to the field of information technology, whereas information security aims to protect relevant information, regardless of the form it takes. The area of information security therefore encompasses everything related to information processing.

In the context of information security and information risk management (ISM/IRM), it is now spelled out more clearly that the business processes concerned must take effect across the entire organisation, and that it is not enough to provide adequate resources to IT operations and application development alone.

The BAIT requirements now clarify, for example, that the institutions must develop a comprehensive training and awareness programme for their staff on the topic of information security.

The BAIT reflect the requirement in the EBA guidelines referred to earlier for a clear allocation of responsibilities by designating additional roles and tasks of information security and information risk management and differentiating them from responsibilities for business processes.

Among other things, the organisational units that are responsible for the individual business processes are responsible for determining and documenting the protection requirements of the relevant processes. By contrast, information risk management is responsible for verifying this determination and documentation.

In light of the complexity of cyber threats, the BAIT now expressly emphasise how important it is for institutions to keep themselves informed about current external and internal threats and vulnerabilities, and to notify the management board about the risk analysis and changes in the risk situation.

The BAIT chapter "Information risk management" now clarifies that threats and vulnerabilities must also be taken into account by information risk management if they could pose risks to the organisation.

Several BAIT chapters address requirements for physical security, as described in the EBA guidelines.

For example, the institutions must develop a physical security policy, implement physical access controls and establish an adequate perimeter protection using state-of-the-art technology. Perimeter protection means protecting the area between the building and the property boundary.

To read more:
https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2021/fa_bj_2108_BAIT_en.html

Transforming risk culture: observations from APRA's pilot survey

- APRA's risk culture survey is internationally leading regulatory practice that expands its supervisory toolkit to transform risk culture.

- Survey results provide a unique employee view of the risk management practices and behaviours in an entity.

- APRA will benchmark up to 60 more entities in the next 12 months, and will share additional insights with industry.

A strong risk culture is essential for effective risk management outcomes that support an organisation's financial and operational resilience.

Ultimately, organisations with a strong risk culture that supports sound risk management practices and behaviours are better placed in terms of financial performance and fair, quality outcomes for their customers.

Under Prudential Standard CPS 220 Risk Management, the boards of APRA-regulated entities are required to form a view of the risk culture in the institution that they govern, and identify any desirable changes to the risk culture necessary to ensure that culture supports the ability of the institution to operate consistently within its risk appetite.

APRA aims to reinforce, support and assess the work regulated entities are doing to build and maintain an effective risk culture. To this end, APRA has introduced an industry-wide risk culture survey recently piloted with 10 general insurance entities.

The survey is a key initiative that supports APRA's expanded supervisory toolkit designed to transform governance, risk culture, remuneration and accountability (GCRA) practices across regulated entities.

APRA's pilot risk culture survey, conducted between March and April 2021, provides insights from employees on perceived risk behaviours and the effectiveness of the risk management structures within their entities.

The responses, over time, will determine the extent to which positive changes to risk culture are (or are not) taking place within individual entities, and correspondingly, will identify areas where an entity's risk culture can be improved.

The survey also provides the opportunity to benchmark results across a number of regulated entities within an industry sector (for example, insurance), providing an opportunity for entity leaders and APRA supervisors to understand how the entity's results compare to others in its peer group.

APRA is one of the only regulatory bodies worldwide that directly collects survey data at an industry level, so APRA's risk culture survey represents internationally leading regulatory practice.

What is risk culture?

Risk culture refers to an entity's attitudes and behaviours towards risk management. Specifically, it is the behavioural norms and practices of individuals and groups that shape an entity's ability to identify, understand, openly discuss, escalate and act on its current and emerging risks.

A strong risk culture creates an environment where employees are comfortable speaking up and voicing concerns with their leaders. It produces better decisions by ensuring a broader range of views are considered, and allows ideas that present heightened risks to be appropriately challenged during decision-making.

It incentivises boards and senior executives to prioritise effective risk management. In doing these things, a strong risk culture helps to deliver better business and customer outcomes for organisations. APRA is committed to enhancing and reinforcing a strong risk culture across all regulated entities.

In particular, an entity's risk culture is influenced and shaped by two key aspects:

- *Risk behaviours:* the observable actions and behaviours of individuals and groups (for example, role modelling, operating practices and symbols, such as discussion of risk management as a standing agenda item in team meetings), and

- *Risk architecture:* the formal structures and arrangements that support the management of risks (for example, systems, policies, procedures and governance structures).

APRA's Risk Culture 10 Dimensions

APRA has developed a framework called the Risk Culture 10 Dimensions to assess the risk culture of regulated entities. The Risk Culture 10

Dimensions articulate the key aspects of an entity's risk behaviours and risk architecture that contribute to its risk culture. Each of the survey questions in the pilot (approximately 40) aligned with one of APRA's Risk Culture 10 Dimensions.

The Risk Culture 10 Dimensions – coupled with the survey results – allow APRA to access comparable data in a consistent way across regulated entities in order to assess and benchmark risk culture.

Figure 1: APRA's Risk Culture 10 Dimensions

APRA's Risk Culture 10 Dimensions is not a prescriptive framework, and APRA does not expect entities to adopt it. While the 10 Dimensions framework provides insights into how APRA assesses risk culture, an entity should have a risk culture framework that fits its own particular circumstances (such as its size and complexity).

This framework should allow an entity to measure, monitor and report on its risk culture in a consistent and meaningful way.

To read more: https://www.apra.gov.au/transforming-risk-culture-observations-from-apra%E2%80%99s-pilot-survey

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 particular individual or entity;

- should not be relied on in the particular 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 with regard to such problems incurred as a result of using this site or any linked external sites.

International Association of Hedge Funds Professionals (IAHFP)

At every stage of your career, our community provides training, certification programs, resources, updates, networking and services you can use.

You can explore what we offer to our members:

1. Membership – Become a standard, premium or lifetime member. You may visit:
https://www.hedge-funds-association.com/HowToBecomeMember.html

2. Monthly Updates – Visit the Reading Room of the association at:
https://www.hedge-funds-association.com/Reading_Room.htm

3. Training and Certification – You may visit:
https://www.hedge-funds-association.com/Distance_Learning_and_Certification.htm