Making the system resilient in a new age of financial services

Financial Services Leadership Summit

December 2019

EY
Building a better working world

tapestry NETWORKS

Financial Services Leadership Summit

December 2019

FSLS

VIEWPOINTS

Making the system resilient in a new age of financial services

We are ten years out and it's not entirely clear to me that people learned the lessons they needed to the last time. Have we really done all that we need to do to understand the risks we are taking on? Have we done enough in the non-financial risk area to understand whether we are going to be resilient going forward?

These questions posed by a participant in the 2019 Financial Services Leadership Summit were central to the discussions on the 16th and 17th of October in Washington, DC. Participants from the Bank and Insurance Governance Leadership Networks – directors, executives, regulators, and other subject matter experts – met to discuss how to make the financial system resilient to a range of evolving risks.

More than ten years after the global crisis, the financial services business has changed, as have the risks of greatest concern to regulators, supervisors, directors, and executives. Large institutions have shored up capital and liquidity, new rules have been implemented, and supervision has tightened. Participants generally say that the regulatory and risk management reforms imposed by regulators and voluntarily undertaken by institutions have been effective.

However, in a shifting environment, new risks are moving up the agenda: operational and technical resilience are increasingly in focus, as are questions about the sustainability of business models and the system's resilience in the face of forces such as climate change and geopolitical volatility. At the Summit, participants discussed the nature of these risks and how they can effectively understand and anticipate the second- and third- order effects to their firms and the system. Keeping up with the pace of change and the complexity of risks in a changing financial services ecosystem will continue to challenge financial institution leaders and their regulators. And pressure on earnings from new sources of competition and a global economic slowdown will challenge risk management and governance.

This *ViewPoints* is organized into the following sections:

The post-crisis regulatory regime may soon be tested

In the decade since the global financial crisis, the financial services industry has made great strides toward shoring up weaknesses in the resilience of individual firms—especially those deemed systemically important—and of the system overall. Regulators around the world instituted sweeping reform agendas, including improving cross-border coordination. The largest financial institutions have improved risk management and oversight and implemented new regulations, including higher capital and liquidity requirements.

> *"There are aspects of the post-crisis reforms that have still not been tested by a true crisis. We still do not know the potential unintended consequences of these untested reforms."*
>
> — Participant

Summit participants largely agreed that these steps resulted in financial institutions that are better positioned to withstand a crisis and a more resilient financial system. A participant said, *"Are we more stable? Can we handle crises better than we could years ago? Clearly, the answer is yes due to all the work done in prevention and in improving the regulatory apparatus."* Yet there are signs that this post-crisis focus on financial risks may soon face its first major test. Several major economies are already experiencing a downturn. Improvements to coordination mechanisms and cross-border cooperation may be under threat as a result of opposition to globalization. A participant said, *"There are aspects of the post-crisis reforms that have still not been tested by a true crisis. We still do not know the potential unintended consequences of these untested reforms."*

At the same time, the financial services sector is undergoing a technological transformation that may introduce new risks that are not well understood and that the regulatory system is ill equipped to address. Some participants questioned whether regulators and other authorities will be able to respond to a crisis emerging from outside the regulated financial sector or stemming from nonfinancial risks, like a major cyber-attack or technology failure.

Summit participants discussed the current state of the post-crisis regulatory reform agenda and the gaps that may remain as the risk landscape evolves:

- **The system is more resilient, but complacency is a concern**
- **A global recession could strain business models**
- **The ability to respond to future crises may be limited**

The system is more resilient, but complacency is a concern

> *"We are certainly now in the process of looking back at a number of post-crisis reforms. We're listening to feedback and making adjustments."*
>
> — Regulator

Post-crisis prudential reforms included new standards to strengthen capital and liquidity, changes to regulatory structures and tools, and enhanced supervision. Participants agreed that large institutions are now better equipped to weather a financial shock, but they cautioned against becoming comfortable that recent measures have fully identified and mitigated systemic risks. Regulators are also recalibrating, with one reporting, *"We are certainly now in the process of looking back at a number of post-crisis reforms. We're listening to feedback and making adjustments. We are looking at simplifying regulations and being consistent."*

More capital and liquidity, less leverage

Two of the most important reforms passed in the aftermath of the financial crisis aimed at shoring up the financial resiliency of large institutions: Basel III in banking and Solvency II in insurance. Final implementation of Basel III has been extended repeatedly and the current implementation date pushed back to January 1, 2022, but today, large banks are generally meeting capital levels that Basel III will require. Nonetheless, leaders and analysts have questioned the relative costs and benefits of these requirements, including trade-offs between safety, on the one hand, the suppression of profitable risk taking on the other.

A regulator observed, *"We have made significant progress in applying the lessons learned since the crisis. Overall, the banking system is in a better and stronger position. Banks have much more capital and and better liquidity.*" A recent EY report noted, however, "There are signs that the consensus on post-crisis objectives is fraying. The implementation of global standards is incomplete and inconsistent across jurisdictions. In some cases, local rules are already subject to review or revision.

New supervisory tools and monitoring approaches

Participants discussed enhanced regulation of systemically important financial institutions and the strengthened supervisory tools and monitoring approaches—some of which have proven effective and some of which remain untested—including the following:

- **Stress testing.** Stress testing, a tool used to measure a bank's capital levels under simulated adverse conditions, has proven valuable to both large firms and regulators in understanding vulnerabilities and in increasing confidence in the resilience of individual institutions to financial shocks. A regulator

said, *"Stress testing has helped to make bank processes internally more forward-looking and also enables us to test banks on how they will handle adverse economic conditions, improving preparedness."* Participants noted how stress testing is adapting to new risks, for example, the Bank of England conducting climate-risk stress tests. A director noted, *"A few years ago, the scenario was another major counterparty going bust, so the Lehman situation was the example. But the more we increased our capital and improved our risk assessment, the better equipped we have become. Through reverse stress testing, we found the only way we could go bust was through several things happening simultaneously: a major macroeconomic or geopolitical issue, plus a major cyberattack or counterparty going bust."*

- **Recovery and resolution plans.** A significant focus of regulatory reform has been the promulgation of recovery and resolution plans, or "living wills," which provide road maps for institutions and their regulators as to how a firm would either wind down or recover from financial distress. Many participants questioned how these plans would work in a real crisis, and the applicability to insurance. A regulator explained how this tool has improved preparedness: *"Asking banks to plan ahead for their own resolution should overcome some of the obstacles that we've seen in the past with resolutions. They ask themselves questions about their structures or new business initiatives and how those would be resolved."* This past summer, the Bank of England announced that it would require all UK lenders with more than £50 billion in retail deposits to publish living wills every two years.[1]
- **New supervisory approaches to identify and monitor systemic risks.** The crisis revealed that both regulators and institutions lacked the capacity to develop a clear picture of risks building up in the financial system. As a result, central banks, which have a broad mandate to maintain financial stability, were given a more prominent role in macroprudential supervision, and new regulatory bodies were created to better gather and analyze data. These include the Financial Stability Oversight Council, established in the United States by the Dodd-Frank Act; the Bank of England's Financial Policy Committee; and the European Systemic Risk Board.

Avoiding complacency

> *"The greatest threat to financial stability is complacency."*
>
> — Regulator

A regulator cautioned, *"The greatest threat to financial stability is complacency. We're working very hard not to be complacent because we do not want to be victims of our own success. Complacency is creeping back into the industry; that's the biggest risk right now. As regulators, how is this experience that we've had going to affect how we manage going forward?"* Another participant noted that while some of these reforms have effectively addressed some types of systemic risks, not all of those identified following the last crisis have been addressed. *"What we see is that we are much better positioned now for an idiosyncratic risk from within the banking sector. But have we solved 'too big to fail'? No. Anyone who tells you otherwise is lying."*

In the current political context, some participants expressed concerns about a rollback of key reforms. One said, *"Capital is much higher. We think banks are much safer as a result, but we also think it would be wrong to suffer from amnesia at a point when you're getting a changing of the guard—people are retiring, people are moving on. Lobbyists are becoming more powerful. We've had significant, albeit discreet, changes to some of the regulatory powers."* An executive shared a related concern: *"Both firms and the regulators have done a lot to rebuild and ensure good resilience, but you worry that things are going in the wrong direction now."* For example, earlier this year, US regulators proposed allowing the largest US banks to produce plans every four years rather than annually.[2]

> *"Have we solved 'too big to fail'? No. Anyone who tells you otherwise is lying."*
>
> — Participant

A global recession could strain business models

While summit participants were generally confident in the financial resilience of the sector, they acknowledged that reforms have largely gone untested. Now, analysts worry that in many economies, an extended period of economic growth will give way to a downturn. With interest rates still at historic lows, there is limited room for central banks and policymakers to respond. A system that has been strengthened over the past decade could soon face its first major test.

Economic indicators suggest that recession is likely

In October, the International Monetary Fund updated its World Economic Outlook report, which noted, "After slowing sharply in the last three quarters of 2018, the pace of global economic activity remains weak. Momentum in manufacturing activity, in particular, has weakened substantially, to levels not seen since the global financial crisis. Rising trade and geopolitical tensions have increased uncertainty about the future of the global trading system and

international cooperation more generally, taking a toll on business confidence, investment decisions, and global trade … the outlook remains precarious."[3] An article in the *Financial Times* noted, "As any number of indicators now show—from weak purchasing managers' indices in the US, Spain, Italy, France and Germany, to rising corporate bankruptcies and a spike in US lay-offs—the global downturn has already begun."[4]

Low rates put added pressure on earnings, creating new risks

The low (or negative) interest rate environment in several major economies not only has left monetary policymakers with little room to maneuver but is creating challenges for financial institutions. Though Fed Governor Jay Powell has indicated that there are currently no plans for further rate cuts, President Trump recently renewed calls for negative interest rates.[5] In the United Kingdom, Bank of England Governor Mark Carney recently commented that rates could be cut close to zero in a downturn, and some analysts are predicting a quarter-point rate cut in 2020.[6]

Participants discussed the problems that persistently low interest rates are causing for firms, particularly by putting pressure on earnings that are already being squeezed by regulatory costs, increasing competition, and soaring technology budgets. An EY advisor said, *"Is this the new normal? New competitors and a low interest rate macro-environment are very difficult for margins. It's putting pressures on institutions."* Low rates threaten banks' net interest margins, while insurers are also exposed through rate-sensitive products like life insurance.

Pressure on earnings could lead to increased risk taking as institutions search for new avenues of growth, particularly in the face of a looming economic downturn. This could also foster conduct issues at financial institutions as they and their customers search for yield. One regulator said, *"You could end up with customers who are struggling to get by and they become less risk averse, and on the business side, companies looking for new sources of profit. I don't think the links between downturns and poor conduct are as well understood as they could be."* The regulator added, *"So much work has gone into rebuilding trust since the crisis. The ability to maintain that trust comes under greater pressure in poor economic conditions."*

"So much work has gone into rebuilding trust since the crisis. The ability to maintain that trust comes under greater pressure in poor economic conditions."

— Regulator

Risks outside of large institutions must also be well regulated

> *"You do wonder if we've been spending too much time fighting the last war and not focusing on the next one."*
>
> — Participant

Concerns about shadow banking surfaced during and immediately after the crisis, but authorities largely focused on addressing risks within regulated institutions. Today, few participants believe that the risks of shadow banking are well understood or controlled. New entrants like fintech and insurtech firms as well as large technology firms entering financial services may also present novel risks that have yet to be addressed by regulation. A participant said, *"The view is that banks have been regulated based on who they are rather than what they do. The issue now is to define what a financial service is and how we define these new models that weren't proliferating in the past. For instance, the concept of stored value has not gotten the regulatory attention I'd expect it to. So getting a handle on who you are versus what you do and how we equate the regulatory burden based on that is important."* A director said, *"You do wonder if we've been spending too much time fighting the last war and not focusing on the next one,"* suggesting that the sources of systemic risk may simply have moved outside of regulatory control.

The continued growth of shadow banking

Some participants noted that more stringent regulations have shifted activity to the less-regulated shadow banking sector. A 2018 Group of Thirty report noted, "Paradoxically, the preventative steps taken to bolster big banks, while welcome, could increase the likelihood that prevention by itself will not be enough given that a corresponding effort was not made with respect to systemically important non-bank financial institutions that could play a bigger role in the financial system as a result."[7]

The FSB defines shadow banking as "credit intermediation involving entities and activities (fully or partially) outside the regular banking system."[8] In the years since the crisis, global shadow banks have seen their assets grow to $52 trillion in 2017, a 75% jump from the level in 2010, the year after the crisis ended.[9] One regulator said, *"Of course we've strengthened the positioning of the regulated financial services sector, but there is still the shadow banking sector, which continues to grow and cause some significant concerns."* Regulators' ability to address these concerns is limited, and policymakers have acknowledged that progress in identifying and regulating potential risks has been limited.

Persistent concerns about a "level playing field" for new entrants

"A level playing field doesn't mean that every business model faces the same type of regulation."

— Regulator

With the proliferation of new entrants in the financial services space, incumbents continue to raise shared concerns that the newcomers do not face the same regulatory scrutiny and could present new sources of risk. Several summit participants noted a lack of a *"level playing field"* regarding the regulatory treatment of new entrants. A participant involved with fintech companies observed, *"There is a perception that fintechs are not regulated. We are regulated; we have to fulfill all the requirements for consumer fair lending, etc. Fintechs are bringing solutions to underserved markets and identifying the places where the customer experience is poor or customers are underserved, and smart people are figuring out how to do it better."*

A regulator clarified, however, that *"a level playing field doesn't mean that every business model faces the same type of regulation. It means the end aims have to be the same—e.g., that consumers are treated fairly—but we might need different kinds of specific regulations. It doesn't mean we should impose the same costs, but that customers should be able to trust new entrants the same as they trust incumbents."*

The ability to respond to future crises may be limited

"It is alarming to see that central banks are more circumscribed in their ability to deal with major crises going forward."

— Participant

In a joint essay published in April 2019, Ben Bernanke, Tim Geithner, and Henry Paulson wrote, "A decade later, the vital question to ask is whether the United States is better prepared today. We believe the answer is: yes and no. There are better safeguards in place to avoid a panic in the first place … But the emergency authorities for government officials to respond when an intense crisis does happen are in many ways even weaker than they were in 2007."[10] The previously mentioned Group of Thirty report came to a similar conclusion, noting, "Of greatest concern, some of the tools available to fight extreme crises, when and if they occur, have been weakened, especially in the United States."[11] A regulator noted, *"The next crisis may have roots outside the financial sector, but we must be able to deal with it within."*

A participant said, *"It is alarming to see that central banks are more circumscribed in their ability to deal with major crises going forward, and there are great concerns about whether they can act how they need to act in the next crisis, which is absolutely coming."* Further, public backlash against the bailouts of financial institutions during the last crisis led to skepticism about the political viability of such actions in the future. A participant said, *"You worry*

about the political costs of a response or if the political capital is there to take action when needed."

Lack of governmental cooperation or global consensus may leave regulators in a challenging position in an emergency. Participants questioned whether the global coordination that took place after the crisis, led by organizations in Basel like the Financial Stability Board, the Basel Committee on Banking Supervision, and the International Association of Insurance Supervisors, would be possible in the future. As one participant said, *"There is increasing uncertainty from an international standpoint. The period post-crisis, where there was close collaboration and consensus on the way to go forward regarding regulations and supervision, seems to be fading."* In the current geopolitical environment in which nationalism and regionalism are increasingly resurgent, this kind of cooperation is difficult to envision. One regulator said, *"We have a clear role to play and mandate, but it's impossible to do it by ourselves. Governments should have a role and be able to intervene when regulators can't manage it alone. But there are questions about how to do that, how to reach consensus and address these issues as a global community."*

***

Summit participants were confident that the regulatory reforms of the last decade have effectively addressed some of the most critical sources of financial risk to the system. They worry, however, that post-crisis calm and macroeconomic growth could lead to complacency and that risks to the system are changing in ways that will make it difficult for regulators to respond. In a recent speech, Wayne Byres, chairman of the Australian Prudential Regulation Authority and former secretary of the Basel Committee on Banking Supervision, said, "The current regulatory framework is not designed for clouds, ecosystems, or partnership models. Not only do we need new skills, additional resources, and stronger partnerships, but potentially new powers to ensure that as critical functions and data move outside the regulatory perimeter, we are able to satisfy ourselves that the requisite level of safety and control remain in place."[12]

Cyber and technology risks threaten systemic resilience

"Going forward, there will definitely be a greater focus on nonfinancial risks."

— Regulator

Operational resilience—the ability of an organization to prevent, respond to, recover, and learn from operational disruptions without harm to customers and the wider market—has become a primary focus of regulators and financial institutions. It is partly driven by concerns about protecting customers from harm, but its primary objective is to ensure the continued functioning of essential aspects of the financial system.

Summit participants discussed emerging sources of nonfinancial risk to individual firms and to the financial system, including ever-more-sophisticated cyber threats and the danger of a major outage that results in a loss of critical services or of data integrity. An executive commented on the wide range of resiliency issues that financial institutions and regulators confront: *"It's cyber, it's continuity of business, it's third- and fourth-party risk management. Everybody is focused on the ability of firms and the infrastructure of the financial industry being able to provide their services in a stress situation."*

"These are harder than things like capital and liquidity, because they involve challenges that permeate the entire organization."

— Regulator

A regulator said, *"Going forward, there will definitely be a greater focus on nonfinancial risks. Cyber risks are a part of that, and operational resilience broadly is becoming more and more important. These are harder than things like capital and liquidity, because they involve challenges that permeate the entire organization."*

These statements reflect concerns from regulators, directors, and executives that the next financial crisis might stem from operational or technical risks.

Sophisticated cyber actors looking to steal and disrupt

The cyber threat to financial institutions and to other critical infrastructure continues to grow, with nation states and other malicious actors staging increasingly sophisticated and destructive attacks.[13] An expert at the Summit referred to a *"cyber arms race,"* noting, *"You have state actors blended in with private actors. Financial institutions cannot handle these types of attacks alone."* Four in five banks now believe that a system-wide industry-level attack or material event is likely within the next five years.[14] A director emphasized the potential severity of the threat to individual institutions: *"You can have a reputational problem or a brand problem, and the bank can lose money. If the bank has a cyber problem, you can lose the bank."* And while the

interconnectedness of the financial system has long been in discussion, a 2018 report from the Brookings Institute on "The Future of Financial Stability and Cyber Risk" noted that the "highly interconnected and tightly coupled" nature of cyberspace means that "disruptions in one area can cascade easily and in unexpected ways."[15] It continues: "interactions between the financial contagion channels and the technological and operational risk channels of cyber-attacks have not been examined carefully. For example, a sustained attack on a large global financial institution could be contagious across both dimensions, but where and how the contagion channels might feed on each other and accelerate risk is an important area for future work."[16]

Major thefts of money and data

"Bad actors are not only trying to access money or steal data, but are [also] trying to destroy data and systems."

— Participant

In July 2016, cyber criminals attempted to steal $150 million from the accounts of a bank in South Asia and later attempted to steal the same amount from a bank in West Africa, using the banks' own systems to issue payment instructions to transfer the money to the attackers' accounts.[17] These attacks showed that cyber actors could not only conduct complex intrusions and manipulate payment systems within a target bank, but also possessed the capability to strike different institutions on different continents within the same time frame.[18] A participant highlighted the implications for controls around the movement of money and data in financial institutions, noting that CEOs often have the authority to move *"seven figures"* on systems that are now being targeted by *"sophisticated, nefarious actors."*

Financial institutions also hold vast amounts of valuable data. Participants are increasingly concerned that the theft of that data could be a larger threat than the theft of money. A Summit participant noted, *"Banks have interesting data, and sophisticated cyber actors want access to that data so they can understand the underpinnings of the financial institution and use that to their advantage for a larger strategic purpose."*

State-sponsored attacks focused on destruction and disruption

Participants highlighted three dimensions of state-sponsored cyberattacks that seek to cause large scale disruption:

- **Destruction of data and systems.** *"Bad actors are not only trying to access money or steal data, but are [also] trying to destroy data and systems. The potential for that is out there. A poll of major banks last year had 26% of respondents noticing an uptick of data destruction in their banks. Data destruction is an important systemic risk,"* stated a summit participant.

- **Targeting the payments system.** A participant observed, *"Bad actors understand the impact of crippling payment systems, especially within nation states."* A participant referenced two attacks on the Mexican and Chilean payments systems as evidence of the *"ability of nefarious actors to get into the payment system itself, to socially engineer the controls. They have the ability to spoof payment messaging, which happens with social messaging, and that allows actors to get into these domains and they can manipulate payment systems."*
- **The financial system as a geopolitical tool.** Because economic sanctions are an important tool used for political purposes, *"the financial sector is in the heart of these national and international security debates—the first instinct for US policymakers is to resort to sanctions and economic measures to punish and to deter and change behavior,"* said one participant. This makes financial institutions an even bigger target for nation states looking to disrupt the financial system.

Why haven't we had a systemic event to date?

For years, experts and network participants have cautioned about the prospect of a major cyberattack within the financial system precipitating a systemic crisis. Summit participants shared two possibilities as to why this has not happened to date:

- **Lack of motivation.** One expert said, *"It hasn't happened yet because the major class of attackers—criminal networks seeking money—are like other deviant globalization actors. They don't benefit from bringing the system down in a profound way. Like parasites, they need to keep the host alive and generating resources so they can continue to skim off the top."*
- **Disincentives for state actors.** As noted, the financial sector is a tool for geopolitics. A participant observed, *"The increasing prevalence of contentious geopolitics means that 'state' actors might have more of an interest in a catastrophic systemic attack in order to severely weaken a geopolitical adversary. Which means the risk is increasing."* Yet, the same participant noted the risks to these actors: *"As with biological weapons,*

> *"The actors most capable of putting the system at risk have not been willing to go that far. 'Responsible' state actors and the ones with most cyber capabilities understand they cannot put the financial system fundamentally at risk."*
>
> — Participant

the ability to 'control' the scale and scope of consequences from a 'systemic' cyberattack isn't confidently high. So, there is more risk of collateral damage than any military thinker would ever want—it's almost, the opposite of a precision weapon, and unintended consequences are very likely, so that reduces incentives as well." These state actors would also risk retaliation. Another participant said, *"The actors most capable of putting the system at risk have not been willing to go that far. 'Responsible' state actors and the ones with most cyber capabilities understand they cannot put the financial system fundamentally at risk. [Large state actors] cannot implode the financial system. There would be huge boomerang effects."*

Loss of critical services or data integrity could trigger a systemic event

While malicious cyberattacks remain at the top of Summit participants concerns, the broader threat to financial institutions from outages or other disruptions could include outages caused by poorly executed systems upgrades and other operational failures, loss of data integrity, and third-, party risks arising from expanding relationships and dependencies on partners and vendors. The high likelihood of significant disruption means that financial institutions need robust response and recovery capabilities.

Prolonged service outages

> *"If a single institution cannot send money out, but can take it in, that could trigger a liquidity issue."*
>
> — Participant

Regardless of the cause of disruption, *"the key question is—given how digitally connected the banking and financial sectors are, and how they face the internet—can the critical availability of a must-run system be there for the financial system?"* asked one participant. Prior to the Summit, participants discussed their concerns regarding extended service outages. An EY advisor said, *"What would be the market reaction? Given the reliance on third-party vendors, what would be the participation required by the interested parties to settle it? If someone has an outage that they don't get out of for 24 hours, what's the impact? What's the behavior? It is not just a black swan event or a cyber event, it's recognizing there is a lot of real estate between a temporary disruption and a disruption where the firm doesn't know when it will be out of it."* A Summit participant outlined a scenario that could trigger a systemic event: *"If a single institution cannot send money out, but can take it in, that could trigger a liquidity issue. At what point do we trust that institution to be able to send money out? We worry about those systemically important payments. When would we create a liquidity crisis by not doing business with them?"*

Loss of data integrity

> *"We worry about those systemically important payments."*
>
> — Participant

Trust in institutions and in the integrity of the information they manage is essential to the functioning of the financial system. A director said, *"The real worry is data corruption. That is the nightmare scenario we should all be thinking about. It's miles above any other concern we have. It's an unconscionable position to find yourself in as a financial institution."* Data corruption could have unforeseen effects that could ripple through the system. For example, a Summit participant said, *"We worry about high-frequency trading and corruption in the data there. Think about a look back that showed there had been a compromise at a key trading group, but they had not seen it at the time. That is difficult to recover from; they might not be able to go back and fix it. And that could undermine the market and destroy trust in key indices."* A director went further, highlighting the dangers of a loss of trust in the data at a major financial institution: *"If the data set at a very large bank is compromised, that could spell the end of the country's financial system."*

The emerging financial services ecosystem presents new risks

> *"Third-party risks are actually fourth- or fifth-party risks, and it is hard to figure out who is at fault when something goes wrong."*
>
> — Executive

As financial institutions enter into relationships with more third parties, they also increase overall exposure to technology risks. When a failure in a vendor leads to a data breach, customers are likely to blame the financial institution to whom they provided the data, and not the related party.[19] Moreover, the third parties' own vendor and partner relationships, which may include data sharing or processing, can be opaque. One participant noted, *"Third-party risks are actually fourth- or fifth-party risks, and it is hard to figure out who is at fault when something goes wrong."*

Concentration could create systemically important entities

In 2014, the University of Cambridge Judge Business School Centre for Risk Studies coined the term "Systemically Important Technology Enterprises." More recently. writing in the *Financial Times*, the Centre's executive director, Michelle Tuveson, said, "What is worrying is the potential for a global system-wide IT failure occurring simultaneously across many organisations—a 'correlated loss' event that affects a vast number of companies, or an entire sector … A number of technology companies has become so deeply embedded in business productivity that they are systemically important to the overall economy … technology enterprises vital to international corporate productivity."[20] An executive observed, *"Cloud providers or companies that*

are providing security software infrastructure, etc.—that's actually where some of the real concentrations are. It's not necessarily that we have concentration with a central counterparty or big bank in the system. Those risks still remain, but it's more us not knowing the technological harms of some of these providers if they fail. It's a new systemic concentration and we need to establish a new framework for understanding it and preparing for a systemic risk resulting from it." As the Brookings report referred to previously notes, the risks from the concentration of these providers are not yet well known: "There is little understanding of the ways in which the failure, whether by accident or adversary design, of an IT company 'too big to fail' (such as a major cloud service provider) might cascade."[21]

One executive observed, *"We are seeing concentration risk with some large, but less innovative providers, but you have a lot of smaller new vendors proliferating, so, we have a new set of problems, but we also must be open to new technology. You definitely do not want to lose access to new technology by being reliant on large incumbent vendors, but you do not want to go from 8,000 to 16,000 new vendors either."*

Could cloud providers be a source of vulnerability?

Cloud computing has rapidly emerged as an area of concern around concentration risk. A few large providers dominate the market for enterprise cloud services: the three largest, Amazon Web Services, Microsoft Azure, and Google Cloud controlled 57% of the market as of the end of 2018.[22] An executive observed, *"[Large cloud providers] set the standard for how data is exposed to the internet. They dictate the terms of protection, so the question is, if your data is ever exposed, who goes back into the cloud system and monitors that?"* A regulator said, *"I used to look at these banks as large and powerful institutions; now I look at their cloud providers and think maybe the banks are not the powerful ones."*

Yet, some participants questioned whether concentration is really any riskier than a more diverse set of providers. One asked, *"I hear all the time that we should be concerned about concentration risk, especially regarding cloud providers. Is it obvious that reducing concentration would improve financial stability? And how would you do it? What would regulators or financial institutions even be able to do about it?"*

Firms are approaching cloud computing with caution, considering ways to take advantage of it without losing control and security of their most valuable systems and data. One executive stated, *"I am an advocate of a hybrid*

> *"If you are going to expose critical data to a third party who has internet access, then you need to make sure your protections are airtight."*
>
> — Executive

approach, because if you are going to expose critical data to a third party who has internet access, then you need to make sure your protections are airtight. You can utilize the cloud, but you need to have a minimum set of standards for providers, such as maintaining encryption keys and ensuring they have good hygiene, in order to protect your data."

While many boards are calling for their firms to move to the cloud and expect substantial data management improvements as a result, firms can and should take precautions: *"I have seen boards touching on two concentration issues. The first is how a company distributes its data and grants access. Data does not have to be congregated in a data lake in a centralized way. It can reside in C2 [military-level] security with a larger security framework around it. The second way is that companies can take their essential data systems that need to be resilient offline, so boards should be asking about that. This kind of discussion inspires boards to have real thinking sessions about what to keep offline and how to do that in a functional and efficient manner,"* said one participant.

Collaborative efforts seek to enhance systemic resilience

> *"Data does not have to be congregated in a data lake in a centralized way."*
>
> — Participant

Summit participants discussed ways in which financial institutions could collaborate with each other and with regulators and governments to mitigate operational and technical risks in the system. A participant noted the challenges for individual institutions in trying to mitigate the potentially systemic implications of a major cyberattack: *"If someone took down State Street or BlackRock from being able to transact, that's going to affect everyone. First order is, you look at shared critical infrastructure, e.g., central clearing parties … Firms are trying to think about it, but I think we have to realize and be humble about challenges like the lack of transparency and our inability to transform the system because we're just participants."*

Industry collaboration

At the Summit, participants were joined by Scott DePasquale, president and CEO of the Financial Systemic Analysis & Resilience Center (FSARC), and Trey Maust, CEO of Sheltered Harbor, to discuss industry collaborations aimed at addressing potentially systemic threats:

- **FSARC.** FSARC was created in 2016 by a consortium of large financial services firms. Its mission is to "proactively identify, analyze, assess, and coordinate activities to mitigate systemic risk to the U.S. financial system from current and emerging cyber security threats."[23] Mr. DePasquale said,

"The key initiative at FSARC is to host a risk committee and bring the government partners and business leaders there to discuss risk-based approaches to running systems and deciding which risks are the most worrisome. We address liquidity issues, data integrity, deposit and payment services, and key credit and liquidity functions. We are worried about liquidity issues or data integrity that would be difficult for the market to recover from... We are worried about the space between the banks, the market infrastructure and the interconnectedness."

"When Sony Pictures was attacked, data was not available at all. If that happened to a bank, that would shake public confidence across the US and the globe."

— Participant

- **Sheltered Harbor.** Sheltered Harbor was launched by large financial institutions in 2015 to establish standards for data backups and resiliency planning so that financial institutions can continue providing critical services following a catastrophic event, such as a destructive cyberattack or another extended operational outage. Sheltered Harbor works with financial institutions to address ways to protect their data on alternative platforms so they can continue providing business services in the event of a large scale attack: "Data has to be survivable, air-gapped and protected. Each market participant, including smaller financial institutions, has to take this approach to make sure their data is protected. There needs to be almost catastrophic insurance coverage for financial institutions," said Mr. Maust.

  Mr. Maust noted that the 2014 hack on Sony Pictures Entertainment served as a warning for financial institutions: "When Sony Pictures was attacked, data was not available at all. If that happened to a bank, that would shake public confidence across the US and the globe. Sony was the watershed moment for us to look at the gaps and vulnerabilities in the financial system." Sheltered Harbor "assumes a breach mentality" —that in order to prepare, firms have to assume a major breach can and will occur—so that "when it impacts your institution, you can recover in your institution and in the industry as a whole," according to Mr. Maust.

Improving collaboration between the public and private sectors

While efforts like the Financial Services Information Sharing and Analysis Center have facilitated information sharing among financial institutions and with the government, some participants called for additional collaboration and support between the public and private sectors. At the Summit two years ago, participants discussed cybersecurity and the potential for the government to do more to assist private sector efforts. At the time, an expert cautioned, *"The cavalry is not coming,"* suggesting governments' efforts were largely focused on protecting their own networks, intelligence, and systems, and that the

private sector would largely have to fend for itself, even against nation-states or state-sponsored attacks. Still, at this year's Summit, a participant highlighted the need for more collaboration: *"The private sector wants to work with the public sector in a different way, but the government is wary of giving a competitive advantage to one institution or sector over the other, and the intelligence community is uncomfortable sharing information. The private sector has to be responsible and diligent about holding the government accountable."*

> *"We are trying to set expectations consistent with industry standards and check to see if firms are meeting those."*
>
> — Regulator

Regulators contend that they are taking active steps to ensure firms are meeting industry standards, but acknowledge their own limitations. One regulator noted, *"The actions firms are undertaking are way beyond what supervisors can do,"* but added, *"We are like auditors and have had no problem finding failures in contingency tests and saying that firms are not meeting those standards. Those things are yielding supervisory feedback. We are trying to set expectations consistent with industry standards and check to see if firms are meeting those."*

A participant encouraged more information sharing and collaboration, while acknowledging the obstacles to be overcome:

> *"We have to recognize that the government is disenfranchised from this problem. We know before they do. They will continue to rely on the operators for early warnings because we operate global systems. Network providers care about keeping networks up and running, but we hear about attribution, yet we cannot go to the government to ask who is responsible, because they cannot help the institutions understand who is attacking them due to legal and security limitations. But the government has a monopoly on intelligence. The intelligence community has to collaborate on this and share information … We had a meeting among the big banks a few weeks ago to talk about this very issue and it is starting to change."*

***

The financial sector is a prime target for malicious attacks designed to steal both money and data, and to disrupt and destroy. As a result, the sector is, in

> *"During the last 20 years, we focused on building moats and firewalls. Now, it is about constant monitoring and system analysis."*
>
> — Participant

many ways, ahead of others in preparing for and defending against attacks or disruptions. But a participant encouraged diligence to protect against cyber and other risks that threaten technical and operational resilience: *"The financial industry, compared to other sectors it is a hardened sector. But we still have to think creatively about the systems. During the last 20 years, we focused on building moats and firewalls. Now, it is about constant monitoring and system analysis. We have to make sure people think creatively about these risks."*

Traditional business models face new sources of disruption

Pundits speak of "Uber or Netflix moments"—times when a new entrant, enabled by emerging technologies, completely upends business models in an industry, fundamentally changing its competitive dynamics and economic performance. Such a moment has yet to arrive for financial services in developed markets despite a host of new entrants and widespread speculation. Fintechs and insurtechs like to position themselves as customer-friendly alternatives to incumbents which offer a more streamlined experience and enhanced digital features. But large banks and insurers increasingly view these challengers less as an existential threat than as potential partners in their own digital transformations. Thus far, the innovators are not taking incumbents off the map, but rather challenging them to improve how they serve customers.

The industry may, however, finally be reaching a tipping point. In comments around the June 2019 G20 Summit in Osaka, Japan, Christine Lagarde, then managing director of the International Monetary Fund, stated, "A significant disruption to the financial landscape is likely to come from the big tech firms, who will use their enormous customer bases and deep pockets to offer financial products based on big data and artificial intelligence."[24] For Ms. Lagarde, Big Tech could bring both significant benefits to the financial system and a "unique systemic challenge to systemic stability and efficiency."[25] Senior leaders of major institutions have historically taken comfort in the idea that, as one director said, *"Big Tech does not want to deal with the stuff incumbents deal with."* Large tech companies like Amazon, Google and Apple have thus far avoided regulation and supervisory scrutiny. But increasing financial services activities in Big Tech – consider, for example, Facebook's foray into payments and digital currencies – suggest that this may be changing. Fundamental disruption of traditional business models is once again a rising concern for senior financial services leaders.

At the Summit, participants discussed the potential sources of business model risk and their implications for firms, regulators, and the financial system.

Big Tech could transform the financial services industry

The debate around the potential role of Big Tech in financial services is by no means new. Western firms and their regulators, observing

"A lot of people are pushing to regulate Big Tech more broadly. If that happens, will the regulatory burden of entering financial service become less of an issue?"

— Participant

the role that Ant Financial and Tencent have played in redefining mobile payments and, more broadly, a revolution in the Chinese financial services industry, have wondered whether similar disruption could take place elsewhere. Now, Big Tech's long-anticipated moves into core financial services are starting to materialize. A participant observed, *"There is a sense that Big Tech has been put off from entering financial services in a big way due to the level of regulation they'd be subjected to. A lot of people are pushing to regulate Big Tech more broadly. If that happens, will the regulatory burden of entering financial service become less of an issue? Would the incentive to enter, paradoxically, be increased by facing a rising level of regulation as a tech firm anyway?"*

Libra brings new urgency to the debate about Big Tech in financial services

"Libra has forced regulators and firms to confront the proposition of Big Tech in financial services."

— Participant

Facebook's declaration in June that it intends "to enable a simple global currency and financial infrastructure that empowers billions of people"[26] via Libra was met with accolades from many in the cryptocurrency community but stiff resistance from leading policymakers. Having observed the struggles of Facebook in trying to gain support for Libra in Washington, a Summit participant said, *"I think it was an interesting announcement. It showed how naïve they are, because everyone was just talking about how they don't trust Facebook anymore and then Facebook comes out and says they want to own money."* While Summit participants were skeptical that Libra would proceed as planned, there was consensus that *"Libra has forced regulators and firms to confront the proposition of Big Tech in financial services."* An executive said, *"You already see partners falling away from Libra. But it has brought a lot of attention to the inefficiencies in the US about how you pay companies and each other; it's very scattered."* While Libra continues to face regulatory hurdles, Facebook appears intent on exploring other avenues in financial services, including via its digital wallet. In comments made at a recent employee town hall, Facebook CEO Mark Zuckerberg discussed plans to allow users to send payments using existing currencies via WhatsApp and Messenger in India and Mexico. These plans, he said, are distinct from the "bigger, or at least more exotic, project around Libra."[27]

Big Tech is already moving into payments and banking

The frustrations of many millions of customers with banking processes, coupled with the treasure-troves of customer data that financial institutions hold, make financial services a tantalizing opportunity for Big Tech. An EY

> *"When you hear how Ant Financial or Alibaba became successful, it was not a plan to disrupt the banking industry; they just created what they knew customers wanted."*
>
> — EY Advisor

advisor explained, *"The products you think about are financial services, but for consumers it's an end-to-end experience. When you hear how Ant Financial or Alibaba became successful, it was not a plan to disrupt the banking industry; they just created what they knew customers wanted. It's the same reason why PayPal and Venmo now exist."* An executive said, *"Facebook, Google, Amazon, and I'll even say PayPal—this is where this will play out. Facebook is trying to catch up with Amazon. The assumption that Amazon doesn't want to touch the regulated sector has held so far. My thesis is that they will hold off as long as they can, but they will ultimately use the rails of the financial system. I imminently expect a proposition from PayPal. I also expect one from Google … I do expect a large tech firm to offer a basic digital bank account."* In fact, a few weeks after the summit, Google announced that it would begin offering checking accounts in partnership with Citi.[28]

If Big Tech enters the financial services industry by leveraging existing infrastructure, it could provide additional partnership or white label opportunities for incumbents but, in the longer term, could also create new competitive threats. A participant observed, *"In payments, Visa was worried about Apple Pay and disruption. In the end, Tim Cook said the payment industry is too hard, so instead of challenging them head on, Apple worked with Visa and MasterCard. I would worry as an insurance carrier about seeing that across the industry. What if Google partners with another major carrier?"*

The "nightmare scenario": incumbents lose the customer relationship

Participants suggested that big tech firms are more likely to siphon off attractive elements of the financial services value chain than to become full-scale financial institutions. The threat of tech companies disintermediating financial services firms from their customers is a concern, however. One insurance participant noted, *"I think taking risks and earning the return we earn in a regulated space can't be that intriguing to Big Tech firms. On the front end of managing the customer experience and potentially being an intermediary between the company and the consumer without taking underwriting risk—we could see them going there."*

Another potential opportunity is acting as an aggregator of financial services rather than the primary provider. *"Think, though, of how many apps people now have to manage finances, insurance products, international and domestic transfers, wealth management, etc. Every transaction has its own app,"* observed one participant, who continued, *"Facebook is actually late to the party—the party is with the aggregators."* In that scenario, much of the valuable

data and direct interaction with customers no longer resides with the financial institutions providing the individual products.

> *"Not a lot of Western regulators would be comfortable with what AliPay and WeChat can do with data across their entire platform."*
>
> — Participant

Reflecting on the mobile payments landscape in China, an executive observed, *"That's essentially the nightmare scenario for US banks. The big Chinese banks are dumb pipes and make money off debt and the float; that's it. WeChat and Ant Financial own the customer and have all the data from people's lives and everything they do. You talk to people there who haven't paid with cash or a credit card in three years. Here in the US, it's so fragmented, it's hard to see exactly how it happens, but I do think it's possible."* Some industry leaders remain skeptical that the "nightmare scenario" could repeat itself in the West. A participant contended, *"Not a lot of Western regulators would be comfortable with what AliPay and WeChat can do with data across their entire platform. They have fantastic data to provide lending services and cross-selling, but I don't think any Western regulator would be comfortable with all of the use cases we're seeing."* The response of US policymakers to Libra may be indicative of the hurdles Big Tech could face in in the West. Within a month of Facebook's announcement on Libra, the US House Committee on Financial Services sent a letter to Facebook's leaders calling for a moratorium on the initiative, citing "serious privacy, trading, national security, and monetary policy concerns for not only Facebook's over 2 billion users, but also for investors, consumers, and the broader global economy."

Digital currencies are gaining traction

Libra has created new dialogue around the potential benefits of digital currencies, particularly those backed by fiat currencies, often referred to as stablecoins. The *Financial Times* recently reported, "When Facebook announced its plans for a private digital payment token called Libra in June, its intention was hardly to goad governments into creating a public electronic currency instead. But that may turn out to be just what it has achieved, by injecting political urgency into a technical debate previously confined to the research papers of central banks."[29] Since the announcement of Libra, Bank of England Governor Mark Carney has issued a call to consider a "Synthetic Hegemonic Currency or SHC to lessen global dependence on the dollar" and "end the benign neglect of the IMFS [international monetary and financial system] and build a system worthy of the diverse, multipolar global economy that is emerging."[30] RBC analysts also commented that the People's Bank of China has "expedited its development of a Central Bank Digital Currency"[31]

"The dollar has nothing behind it—the gold standard is gone. We now believe in currencies that have no support. It's a new paradigm."

— Participant

and that, "If US regulators ultimately dismiss Libra and decide not to draft regulation to encourage Crypto innovation in the US, China's [Central Bank Digital Currency] may be strategically positioned to become the de facto global currency in emerging economies, largely through Alipay, WeChat, UnionPay and other messaging and payment apps."[32]

A sovereign-backed digital currency that achieves mass adoption would represent a fundamental systemic disruption and could challenge the US dollar. A participant said, *"Firms need to be seriously looking at this. The dollar has nothing behind it—the gold standard is gone. We now believe in currencies that have no support. It's a new paradigm."* One director offered a historical perspective, *"A thousand years ago coins were being used. If we think about the dominance of the American currency, it's only been 70–90 years, so there's not much history. It's inevitable that there will be something else in the future and we have to think about it. But in this complex transition period, it's still the only currency you can trade around the world."* China's intentions, meanwhile, may not be so ambitious. A participant noted, *"China is a giant sandbox thanks to capital controls. I can see the issuance of a digital currency directed by the government, but at this stage, I'd stay away from saying the aspiration is making it the emerging market currency. I don't think they'll aim that high from the get-go."*

Incumbents must get ahead of potential disruption

Financial services firms and regulators are grappling with appropriate responses to the potential disruption posed by Big Tech and emerging technologies. A director observed, *"Figuring out how to manage through all of this in the context of a new wave of privacy concerns, emerging issues with geopolitical management, and developing regulations—I think that's where all of us, including the new entrants, will have to rethink and adapt our strategies."* Senior leaders are contemplating a range of options:

"China is a giant sandbox thanks to capital controls."

— Participant

- **Be the disruptor.** Some are convinced that incumbents must intensify their transformation efforts, but doing so requires them to develop new, more agile cultures, structures, and capabilities. A participant said, *"It's not impossible for insurers to disrupt themselves. The issue is trying to figure out what to do with data from AI and machine learning, how you can use that data and then build predictive tools for the business. It's possible, but then you also need to have a mindset to let a bunch of these kids loose to be useful to the business."* Another participant stressed that finding the

right people to participate in and lead transformation is crucial: *"It gets back to talent. We need the talent to make the pivot."*

- **Partner with start-ups and tech companies**. Partnering gives incumbents access to emerging technologies and different sources of expertise and different kinds of customer interactions. It also allows them to learn how to think and act like a challenger. One participant stated, *"We do a lot of joint ventures with different technology platforms, but you need to have a tone at the top that you are willing to fail, learn lessons, spend more money on other things, and work across silos. The CEO has to push that mentality. What has worked well for us is that investment dollar amounts in these startups can be very small."* Identifying and partnering with the right startups remains a challenge and a potential source of competitive advantage. One participant noted, *"The threat of insurtechs is that my competitors will adopt them, and then I will not just be fighting these little ants."* Despite the competitive threat from big tech companies, many financial institutions are also partnering with them, for example Goldman Sachs with Apple, Citigroup with Google, and JPMorgan Chase with Amazon.

- **Adapt to external technological changes**. Some technologies may force incumbents to fundamentally change existing practices. The Internet of Things (IoT) and the emergence of autonomous vehicles, for instance, are altering the risk landscape for insurers, pushing them to consider new business models. IoT devices generate vast amounts of data, permitting new kinds of risk mitigation. Regarding self-driving cars, one participant noted, *"We operate on the prediction that at some point cars won't crash; we'll reach an inflection point where insurance for cars will start to shrink."* At the same time, self-driving vehicles will pose new risks, perhaps shifting liability from drivers to the software that controls them and thereby creating the need for new kinds of insurance cover.

***

Some participants are pessimistic about the ability of large, Western incumbents and their regulators to keep pace with these rapid changes, which are often emerging faster elsewhere in the world. A participant lamented, *"I don't think we will be able to stay on the leading edge of innovation in the US, and I think we'll lose banking power for that reason."*

Building sustainable, responsible financial institutions

Just as financial institutions are closely linked to the broader economies in which they operate, a range of exogenous factors can influence their performance, including geopolitical volatility, shifting social norms, and climate change. Climate change and broader sustainability issues, in particular, are moving up the agenda for the leaders of financial services firms. Commitments to sustainability are no longer merely a matter of corporate citizenship; sector leaders recognize that sustainability-related issues can pose substantial financial and reputational risks. This is true both for individual institutions and the sector as a whole – as one participant stated, *"If we don't have a sustainable planet we can't have a sustainable financial system."*

The growing sustainability imperative

Though the concept of sustainability often encompasses a range of social and environmental issues, climate change looms especially large among sustainability issues in financial services, and leaders across the financial sector are increasingly recognizing climate change as a source of systemic risk. In a November 2019 report, for instance, the Financial Stability Institute of the Bank for International Settlements declared that "In previous financial crises, events once deemed implausible have materialised. Climate change poses the same threat."[33] One summit participant urging other to think through the potential impact of climate change on the financial system, identified it as one of the *"existential risks facing our entire society."*

The nature and scope of climate risk

The impact of climate change materializes through two primary channels: physical risk and transition risk. Physical risk refers to the direct impact of a warming climate, such as damage from more frequent and more severe catastrophic weather-related events. It also includes more gradual changes such as rising sea levels, increasing frequency of floods, wildfires, and droughts, and public health dangers created as a result – for example, the spread of mosquito-borne diseases. The insurance sector faces several direct effects of physical risk: increased property damage will be felt by insurers in higher claims and by policyholders in higher premiums, while failure to adapt risk models to a changing environment could result in severe and unexpected losses. More broadly, climate change increases the likelihood of asset devaluation in areas sensitive to climate risk, resulting in loss of collateral and

asset values for a range of financial institutions.[34] A recent study concluded hat, by 2050, sea level rise will subject land that is now home to 300 million people to annual coastal flooding, while daily high tides could rise enough to cover land currently occupied by 150 million people.[35] In October 2019, Morgan Stanley estimated that $56 billion in commercial mortgage-backed securities are exposed to coastal flooding risk in the United States alone.[36] A global temperature increase of two degrees Celsius could result in a doubling of mortgage losses in the United Kingdom.[37]

"We all say it's a long-term risk, but I'm not sure we'll have a long time to adapt."

— Participant

Transition risk stems from efforts to mitigate climate change and transition to a low-carbon economy, spurred by policy, technological developments, or public opinion. The realization of a low-carbon economy could result in stranded assets in carbon-intense sectors. Material and large-scale devaluation of assets could in turn have a significant impact on the balance sheets of financial institutions, with broader implications for the financial system. The scope is potentially vast; studies have estimated the losses associated with the devaluation of assets as a result of transitioning to a low-carbon economy could be as high as of $20 trillion.[38]

The near-term effects of climate change

One summit participant said, *"We all say it's a long-term risk, but I'm not sure we'll have a long time to adapt."* Evidence of increased economic losses from climate change has already emerged. Costs associated with natural disasters have exceeded the 30-year average for seven of the last 10 years, and the number of extreme weather events has tripled since the 1980s.[39] In particular, property and casualty insurers and reinsurers are seeing increased losses from extreme weather events, floods, and wildfires. Insurance losses from climate-related weather events have increased fivefold during the last few decades.[40] The years 2017 and 2018 saw combined global insurance losses from natural disasters that hit a record $219 billion.[41]

While most of the current impact comes from physical risk, the effects of transition risk are also beginning to materialize. A recent report from the Federal Reserve Bank of San Francisco, for example, concluded that "even long-term risks can have near-term consequences as investors reprice assets for a low-carbon future."[42] Indeed, decisions made in the coming years in this area may have implications for not only firms' reputations, but also for the financial system more broadly. One participant said, *"The effects of climate change on the global economy must be discussed. History is being written tomorrow, but the future is being written today with regard to that risk."*

Financial exclusion and government intervention

> *"It's a serious question for the industry: How do you participate and offer reasonable protection at an affordable price?"*
>
> — Director

Climate change threatens to hinder access to financial services. For example, a recent report from the Federal Reserve Bank of San Francisco concluded, "There may be a threat to the availability of the 30-year mortgage in various vulnerable and highly exposed areas," which will disproportionately affect low-income communities.[43] Similarly, the Bank for International Settlements warned in a 2019 report, "On financial exclusion, as insurers become more aware of their climate risk exposures and are better able to quantify the risks, they may end up raising premium rates or withdrawing coverage from certain business lines or geographical areas."[44] One insurance director said, *"What do we do with uninsurable risks? How do we engage with governments around that? There is a lot of work that needs to be done in this area."*

Indeed, the retreat of financial institutions from risk-prone areas raises the specter of further government intervention. One director said, *"We are running into a situation where cost is becoming so high that the private industry cannot underwrite it; then it becomes a socialized cost of the state or a nation. It's a serious question for the industry: How do you participate and offer reasonable protection at an affordable price?"* This dynamic is already beginning to play out in some areas. As insurers reduce their exposure to wildfires in California, the insurance commissioner of California, Ricardo Lara, has asked the legislature for power to compel insurers to write insurance in those locales. At an August 2019 meeting he said, "We want lawmakers to give us the authority to say that you have to, as an insurance company, write in these communities, because people have done what we've asked them to do: harden their homes, get that defensible space."[45]

Incorporating sustainability into policy and regulatory mandates

Central banks, policymakers, regulators, and supervisors are beginning to view responding to climate risk as a central part of their mandates. Central bankers increasingly argue that climate risk poses a threat to financial stability, noting potential transmission channels and feedback loops between the financial system and the effects of climate change in the real economy. One participant observed, *"Central bankers are worried about climate change. I think that's the big kahuna going forward. It will be the focus of much central bank effort in the future."* Another participant noted that *"the EU is taking this seriously. The sustainable finance action plan has been*

"The objective is to reorient capital flows to sustainability, mainstream sustainability into risk, and foster transparency with disclosures."

— Participant

instituted. Its objective is to reorient capital flows to sustainability, mainstream sustainability into risk, and foster transparency with disclosures."

One regulator described the challenge of incorporating climate change into its oversight, given the long-term nature of the risk: *"As we've looked at how climate risk fits into our supervisory mandate, we struggle with how to rank it with regard to most of the major risks we focus on, which are more short-term risks, whereas climate change is a bit longer."* Some regulators also question their role, as one acknowledged, *"We haven't been forward-leading the charge, but we are engaged. We're more in follow mode than leader, that's fair to say. The more it's talked about out in the public and meetings like this, we will have to engage."*

Nevertheless, supervisors are asking financial institutions to incorporate sustainability into their risk management frameworks in a number of ways:

- **Increasing climate-related disclosures.** In 2015, the Financial Stability Board established the Task Force on Climate-Related Financial Disclosures (TCFD), which released its initial recommendation in 2017. It identified four areas of disclosure for climate-related risks: governance, strategy, risk management, and metrics and targets.[46] By 2019, 785 organizations had become supporters of the task force, including many of the world's largest banks, asset managers, and pension funds, managing assets of $118 trillion.[47] One participant stressed that *"TCFD has to be top of mind"* for financial institutions. Another participant cautioned that the development of disclosure metrics is still a work in process: *"We need to get some consensus on metrics—that's a major step."*

"We need to get some consensus on metrics—that's a major step."

— Participant

- **Including climate in risk management frameworks and capital regimes.** Several supervisory authorities have proposed integrating climate risk into institutions' risk assessment frameworks. The European Commission is exploring the feasibility of including climate-related risks in banks' capital requirements.[48] The European Insurance and Occupational Pensions Authority (EIOPA), recognizing that few insurers currently account for climate change when calculating liabilities, recently urged insurers to embed long-range climate scenarios in their risk management and their own risk and solvency assessment processes.[49]

  While there has yet been little support for incentivizing environmentally friendly investments by lowering capital requirements, some prudential regulators are considering taking into account the increased market or credit risk imposed by "brown" investments. For instance, Bank of England Governor Mark Carney recently noted, "We would be more open to a

'brown'-penalizing factor, if you will, because something that is quite damaging, quite polluting, one would expect at some point that there would potentially be some adjustment of regulation for that. And a consequence of that would potentially be higher risk."[50] Similarly, one participant pointed out, *"One thing being debated in the EU is whether to introduce environmental compliance as a variable in public procurement."*

- **Stress-testing.** Several supervisory authorities, including the Bank of England, the Banque de France, and EIOPA, have begun—or announced their intentions to begin—to integrate climate change scenarios into their stress tests for financial institutions. One participant encouraged directors to ask, *"Has your bank put together a report on how you'd do climate change analysis and stress-testing? If you do so, you will find gaps in training and personnel and operations."*

Social pressure is increasing

> *"Societal expectations of firms are changing … how you respond to those shifting expectations could have crucial impact on your ability to retain trust and avoid or ride through the next crisis."*
>
> — Participant

Financial institutions face pressures from constituencies that go beyond policymakers and regulators. One director said that leaders of financial institutions devote attention to sustainability issues *"Because our stakeholders insist. Because as people we care. And because there are political pressures forming as well."* Another participant noted, *"Societal expectations of firms are changing, including the expectation that firms will have greater social conscience. I think how you respond to those shifting expectations could have crucial impact on your ability to retain trust and avoid or ride through the next crisis."* The pressure can become intense. One director recalled the pressure a bank faced to discontinue lending to the private prison industry: *"We've had protesters going to branches, assaulting customers, etc. We thought we could wait it out, but it persisted. We were basically bullied on this point."*

Incorporating sustainability into financial institutions' operating models

External pressures and internal convictions are pushing boards and senior executives toward acting as stewards of responsible financial institutions. While financial institutions have at times downplayed the potential impact of climate change, that seems to be changing. One participant said, *"Some insurers have said they can just reprice things as necessary, but I don't know about that. The pricing issue has a lot of limits. You can now see that some risks linked to climate change are not insurable.*

"We're seeing big commitments by firms that are actually tough to execute in reality."

— EY Advisor

Climate change is at the heart of the risks for the future of insurance." Indeed, concerns about climate change has risen to the top of the agenda for insurers. A survey released in October 2019 found that climate change was the most-cited emerging risk for insurance actuaries, with 22% identifying it as the leading risk.[51] Another participant noted that *"I've been working in climate change for over 20 years, and in the last year the increasing interest across the firm and outside it has been amazing."*

Making public commitments

Recent years have seen an array of initiatives designed to encourage financial institutions to build sustainability into their operations. The United Nations Environment Programme Finance Initiative has spearheaded the establishment of the Principles for Sustainable Insurance (PSI), and the Principles for Responsible Banking (PRB) which formally launched in September 2019. Within a broader framework of sustainability, these principles aim to position the insurance and banking industries to contribute to climate change mitigation and adaptation.[52] To date, over 70 insurers have signed on to the insurance principles, while 130 banks representing $47 trillion in assets have signed on to the banking principles.[53]

"The industry has been focused on this in the United States and has made changes in its lending practices in response to climate change."

— Director

A number of financial institutions have made commitments to exit relationships with entities that have carbon-intensive operations. For example, nearly 20 major insurers have announced commitments to limit or discontinue underwriting the coal industry. The UN-backed Net-Zero Asset Owner Alliance, an alliance of pension funds and insurers responsible for a total of $2.4 trillion in investments, announced a commitment to achieving carbon-neutral investment portfolios by 2050.[54]

Some participants shared skepticism about signing on to such initiatives or making public commitments. A director said, *"It's rhetoric over action."* Moreover, an EY advisor cautioned institutions to ensure they can meet their stated goals: *"We're seeing big commitments by firms that are actually tough to execute in reality."*

Citi is the only major US bank to sign on to the Principles for Responsible Banking. Similarly, as one participant noted, no US insurers are among the more than 30 insurance companies to have signed on to the Principles for Sustainable Insurance, and Chubb is the only United States-based insurer to commit to no longer insuring or investing in coal.[55] Summit participants pointed out, however, that geographic disparity may not be as great as it appears. *"Banks have a fair amount of disclosure around climate risks. The industry has been focused on this in the United States and has made changes in its lending*

practices in response to climate change, for example. If you're looking for rhetoric, maybe it's not there, but the actions are there," according to one director.

Balancing stakeholder interests

> *"Long term, we need to be convinced that they're moving in the right direction toward a more sustainable model. We're trying to influence clients over time rather than just deciding, 'OK, we're out right now.'"*
>
> — Director

While divestment is becoming more common, participants cautioned that such efforts are complicated and require nuanced decision-making. One bank director said of a bank's decision to cease lending to coal-related projects: *"It was a very difficult decision. Ultimately, it made sense for our broad base of constituents, but it was not this clear-cut moral decision some might paint it as. There are a lot of factors. You have to look across your constituents and make a call."* Another director said, *"I've been in boardrooms where we've discussed individual issues like this where you may have to make a hard decision. You have to look at these issues from many angles. Guns, for instance. Could it hurt you losing the customer? Sure, but you're probably doing it for other reasons that are worth the short-term impact."*

Some participants advocated efforts to engage with clients to influence decision-making, rather than exiting those relationships. *"We approach it through engagement. We try to understand if the company is diversifying, modeling their own scenarios, etc.,"* said one participant. *"Or are they just closing their eyes to all this and just pretending it's not happening?"* A bank director shared, *"One approach we're taking is an attempt to analyze our institutional clients. Long term, we need to be convinced that they're moving in the right direction toward a more sustainable model. This is going to be difficult to execute, but we're trying to influence clients over time rather than just deciding, 'OK, we're out right now.'"*

Whatever the approach, for sustainability initiatives to be successful, they will need to be driven by key leaders at the organization, a participant said: *"You all have teams working on this at your firms, but it has to go from silos and get more engagement at higher levels. It cannot be a side project."*

Geopolitical risks: shifting United States policy towards China

"The biggest risk right now is that the geopolitical system has changed quite fundamentally in the last decade. The political interactions and rules-based operations have been ripped up. It's a systemic risk because you get the sense that the entire game is changing," stated a risk executive. Nowhere is this more evident and more significant to the global economy than in the US-China relationship. At the Summit, participants were joined by Ely Ratner, executive vice president and director of studies at the Center for a New American Security, for a discussion on how that relationship is evolving and what will define it in the future. Mr. Ratner described a *"profound shift"* in US policy toward China, increasingly defined by *"a deep, structural, strategic competition"* between the two countries. He said this policy in the US *"is not driven by Trump, and will endure well beyond Trump. Tariffs and trade are just a distraction, a minor piece of a much deeper structural strategic competition between the two countries."* Mr. Ratner described the drivers of this competition:

- **Unmet expectations.** For the United States, the more hawkish stance towards China is rooted in dashed expectations that the "Middle Kingdom" would adopt Western political and economic models over time. *"China hasn't met expectations that it would open up politically, that the economy would open up with a diminished role for the state, that they would accept the US security order in Asia, that they would increase participation in the international order,"* Ratner observed.
- **Rising global ambitions.** At the same time, China's view of its role in the world has also changed. According to Ratner, *"Wars in Iraq and Afghanistan and the global financial crisis increased the speed with which China saw its own rise relative to the US."* As a result, he explained, Chairman Xi's goal is a *"China-led, illiberal sphere of influence."* The question is *"how illiberal and how expansive."*
- **Fundamental opposition.** Ratner believes that *"there is no grand bargain to be had, no strategic equilibrium will be reached. The dominant frame [in the United States] for the China relationship is now*

Geopolitical risks: shifting United States policy towards China

competition. There is no aspiration for a special relationship. Economic interdependence is no longer viewed as a source of influence over China." There are signs that an economic "decoupling" is underway, although questions remain as to how far it would go. According to Ratner, *"A year ago, people said 'it can't happen,' now it has started. US actions around Huawei, for example, are reinforcing China's desire to build their own technology."* Nevertheless, China will likely continue its efforts to draw in foreign expertise to help critical industries advance. According to EY Asia-Pacific Financial Services Regional Managing Partner Gary Hwa, *"China is accelerating opening its domestic markets and might use the tensions with the US to open up the financial services sector. The key reason is to create competition and to gain expertise."*

Risk governance adapts to a changing risk landscape

Following the financial crisis, supervisors, boards, and management teams focused heavily on enhancing risk management and board oversight of risk. Much of their effort went toward developing risk appetite frameworks, addressing risk culture, and refining the working of board risk committees. As outlined in this *ViewPoints,* the nature of risk has changed since then; in particular, non-financial risks, which have always been more challenging to model and embed in risk appetite frameworks, are more prominent. The competitive landscape is crowded with new entrants and new partnerships and vendor relationships. Exogenous risks resulting from a volatile geopolitical environment and emerging issues like climate risk are increasingly concerning to boards. At the Summit, participants considered whether the post-crisis focus on risk governance has adequately addressed these evolving risks.

One director stated, *"In our boardroom and in the institutions I'm familiar with, the lessons of 2008 and 2009 remain very much on the top of our minds."* But participants also acknowledged the challenges in adapting risk governance to the current environment. As they stare down a potential economic slowdown, boards will need not only to understand new threats to their institutions, but also to remain vigilant about traditional financial risks and internal control problems. A director asked, *"Have we really done all that we need to do to understand the risks we are taking on? Have we done enough in the non-financial risk area to understand whether we are going to be resilient going forward?"*

This section of *ViewPoints* is organized around the following:

- **Boards must remain vigilant under pressure**
- **Non-financial risks will continue to challenge board oversight**
- **Effective oversight requires substantial time and new sources of expertise**

Boards must remain vigilant under pressure

Financial institutions are operating in a persistently low interest rate environment with a potential economic slowdown on the horizon. At the Summit, participants discussed the need to ensure that standards, such as those around loan covenants and underwriting, remain high as firms seek new ways to improve margins.

Earnings pressures could challenge risk appetites

> *"You have to prepare for a decrease in loan demand and a deterioration of terms, which is even more challenging for risk management."*
>
> — Executive

An executive noted the dual impact of an economic downturn for banking: *"Not only does lending go down, but the quality of the lending goes down. There's more stretching for yield, and we've talked about the unintended consequences of that. You have to prepare for a decrease in loan demand and a deterioration of terms, which is even more challenging for risk management."* These pressures could strain the agreed risk appetite, as business units seek growth opportunities. The same executive predicted, *"We will see limits being challenged because product lines will stretch to go down market or stretch core competencies."* This executive encouraged directors to watch for creep as businesses seek new opportunities or chase trends, suggesting they consider, *"Wait a minute, do we know what we're doing in this area? I know there's money there, but are we good at this?"*

One director said that while they had not seen evidence that standards had diminished, some firms were now competing more heavily on price. This participant said, *"The question is, as directors, are we comfortable with cutting price? Those earnings are critical for withstanding stress and losses."* Another described the balance that directors must strike: *"We hear continually about deals that go to someone else because of covenants. On one hand, you're happy we didn't do it, but you wonder where we are doing it. And if those standards are being lowered elsewhere in other firms, you could end up with the risk back inside your portfolio, so you don't know that you are protected from it anyway."*

Considering sources of concentration risk

> *"We are spending more time on concentrations, looking at pockets of similar activity and similar risk-taking in different parts of the bank."*
>
> — Participant

Participants are also looking more closely at issues like concentration risk, including across traditional risk silos. One participant reported, *"We are spending more time on concentrations, looking at pockets of similar activity and similar risk-taking in different parts of the bank that you wouldn't normally link. A lot of what we are trying to do is get away from looking at classical business lines, getting away from traditional risk categories, focusing much more on types of concentrations across them that are not so obvious."*

Another participant outlined the ways that their institution takes systemic concerns into account: *"We are underwriting with resilience to potential stressful scenarios in mind, to ensure we are resilient enough to be profitable under stress. I am sure most firms are doing this. And then in the risk appetite framework, one can think about concentrations. So, we're going to keep participating in an area where we may see growing risk, but not let it get unduly large … The hard part is imagining and seeing around the corner to all*

the nonobvious ways these risks can bulge out and impact you in a second- or third-order way."

> *"Things that we are more familiar with—capital erosion, loss of liquidity—we understand. The problem with the operation side is that we don't know how severe it could be."*
>
> — Participant

Addressing costs without creating additional risk

With earnings under pressure, firms are continually looking to control costs. But as a participant noted, *"It is very difficult to reduce costs: cyber is not going away, so you cannot cut expenses there, AML and related compliance costs are not going away, so you can't cut back there, digital transformation is not going away, so you can't reduce your spending there."* This means that firms *"need to retain the same level of diligence, but do it smarter,"* by leveraging robotics, AI, and machine learning to automate and improve processes, according to one director. *"You have a lot of risks now,"* an EY advisor noted, *"but you have tech that allows managing those in a way never done before. For example, you can move from sampling to complete testing. There is a positive story here, but you need a willingness to tear up what is done today and do it differently."*

Non-financial risks will continue to challenge board oversight

Most directors and regulators expressed confidence in the actions institutions are taking to improve management and oversight of traditional financial risks—market, credit, and liquidity, for example—despite their concerns about economic and market pressures. Non-financial risks may be a different matter. One participant reflected, *"Thinking about non-financial risks, are we applying the lessons learned? Is the flow of information effective in making sure that we are prepared for the next crisis?"* For individual banks and supervisors alike, there is limited information available to identify the operational risks that could ultimately create systemic stress. *"What are the things that could happen that could be really severe? Things that we are more familiar with—capital erosion, loss of liquidity—we understand. The problem with the operation side is that we don't have examples. We don't know how severe it could be. When I look at cyber, loss of data, we've yet to accumulate the data to tell us what the severity will be,"* reported another summit participant.

> *"The risks being faced have evolved substantially in the last five years and the overall amount of risk firms face has gone up."*
>
> — EY Advisor

An EY advisor highlighted the results of their recent risk survey conducted with the Institute of International Finance (IIF), noting, *"We have seen a significant increase in the non-financial risks that institutions are facing. The risks being faced have evolved substantially in the last five years and the overall amount of risk firms face has gone up. Most organizations today feel good about*

where they are with financial risks but are clearly focusing on the non-financial risks and still figuring out how to manage them."

Continuing improvements to oversight of cyber risk and operational resilience

The EY/IIF report notes: "Five years ago, in 2014, cybersecurity did not even make the top 10 priority list for either [CROs or boards]. Now it's by far the most significant risk and has been at the top for three years in a row. No other risk comes close."[56] Many directors remain concerned about ensuring that their institutions are taking all necessary measures to protect themselves from an idiosyncratic or a systemic cyber-attack. A director observed, *"We are spending money and engaging frequently with management and with peers on this. Yet this is a war, and wars are decided by battles. But with this, when the battle takes place, it is too late. What should we do as board members to be sure we are taking all preventative measures?"*

Participants discussed steps to improve governance of cyber and operational resiliency risks:

- **Diligence around basic hygiene.** A participant noted that a lot of operational issues often boil down to a lack of *"good hygiene"* around IT: *"IT is often the root cause of a lot of problems in financial institutions. So, while there is not a specific set of standards, there are things directors can be asking about: whether your systems are out of date, when they are patching, are there segregation of duties? You'd be surprised, if you ask the right questions what you hear back. It's not where people want to spend their time and energy, it's consuming and costly, but it's absolutely where if you're not doing it it's where the problems and root cause comes from. It's the old stuff, not the cutting-edge stuff. You don't need to be a tech expert."* Many participants agreed, and one reported that even more mundane issues require diligence: *"I asked a cyber expert, 'If you were going to attack us, what's the first thing you would do?' They said, 'Steal an employee's access card.'"*

"Most vulnerabilities are in the seams within an institution that you are not seeing until it is too late."

— Participant

- **Understanding the institution's data strategy.** A participant stated, *"The board has to understand the data architecture of the company, how the institution acquires and uses data, and what sort of fraud protections are in place to safeguard the data."* A director noted that these discussions lead to fundamental questions: *"How does this influence how we think about data acquisition – what we want and its relative value – and what it means to protect it and what is the risk of losing it?"*
- **Ensuring sufficient testing and training.** *"Boards have to be privy to penetration testing and accompanying training through exercises and system testing to understand what kind of threats can emerge. There needs to be a clear understanding of how the institution addresses problems when things do occur,"* stated one participant.
- **Understanding third-party dependencies and potential weak spots**. The expanding financial services ecosystem is drawing more attention to third party risk management, as vendors and partners are increasingly handling sensitive firm and customer data. As a result, boards are asking more questions about these relationships. A participant said, *"You need to be sure management is asking key vendors about their cyber practices and whether they are concentrating that data."* Another observed, *"Most vulnerabilities are in the seams within an institution that you are not seeing until it is too late, like third-party vendor risk. You have to test the seams within your enterprise, being careful about where third parties spend to protect their infrastructure etc."* A participant predicted that the robust approaches adopted for anti-money laundering and know-your-customer diligence would migrate to managing vendor due diligence.

Monitoring the rapid spread of (mis)information

In a discussion earlier this year, the chair of a financial institution said, *"The power of social media today is exponentially greater than even two or three years ago. It's like a snowball going down a hill. It keeps getting bigger. It changes behaviors. It can create a false truth at scale very quickly. Most institutions probably haven't thought defensively about just how pervasive it is today."* Recent studies suggest that around 3.5 billion people, some 45% of the world's population, actively use social media.[57] Another director noted the broader impact on society: *"Social media is also changing traditional media. Newspapers react as fast as they possibly can with no regard for standards."*

> *"Reputation is another thing that can kill a financial institution if you get it wrong."*
>
> — Director

When asked what might trigger a future crisis, one participant predicted, *"The loss of confidence of our customers and depositors in the world of social media. That's really about confidence in the system. People talk about cyber being a trigger. How quickly will we lose confidence in an organization to figure out what the problem is and be trustworthy again?"*

Boards are engaging in different ways to understand the potential risks and how their institutions are managing them. One director reported, *"I now have frequent conversations with our reputation risk officer. So, in effect, a Reputation CRO. Because reputation is another thing that can kill a financial institution if you get it wrong."* Another said their firm had adapted governance and reporting processes in response: *"At our cyber center we also have people monitoring social media. We monitor social media from the customer and employee perspective. But things escalate very quickly internally, for example if someone at a branch says something or does something inappropriate. It amazes me how the firm has been trained to process that and ensure senior management can respond before it blows up and gets ugly."*

Improving response planning

> *"It is the newer areas like reputation risk and operational risks where we tend to get a lot of information and where it can be difficult to cut it down to a few key metrics."*
>
> — Director

Regardless of the type of incident—whether a cyber breach, a service outage, or a negative report in the traditional media or social media—a participant stated, *"The most important part, and where you can really put yourself at risk, is the choices you make about how to respond. Take any case study on this, where it's a detection and response, the bad stories are when the choice of response was really bad. So, the state of readiness for the critical response team is very important."* Another participant noted the persistent weaknesses in some firms' planning efforts: *"I've been surprised that some of these playbooks have been more about controlling what to say and who to say it, but not about how quickly and effectively you respond."*

The board has an important oversight responsibility in this regard. One EY advisor asked, *"Do you know the person responsible for responding? Do you know the team, and have you seen them in action? Have you conducted a postmortem on a previous issue?"*

Effective oversight requires substantial time and new types of expertise

In the years since the crisis, many boards have met more often, with regular conference calls between board meetings, and they have reviewed massive amounts of information from management. Overseeing the vast array of non-

financial risks that financial institutions now face means that the time required of directors to stay on top of critical issues and understand the nature and quantity of risk their institutions are taking on has become very high. As the nature of risks changes, so too do the desired skills and experiences for board members.

Getting the right information to the board

Board books, and particularly risk committee reports, swelled in the years after the crisis. Over time, many board leaders told management to avoid overwhelming the board with so much information that key risk indicators could be obscured. As the range of significant risks faced by financial institutions expands, this tension remains. *"It's a never-ending battle in that regard. I think, as a director you get overwhelmed with information, so then you go through a cycle to get presentations focused and more forward looking, but it always starts to drift,"* reported one risk committee chair.

In traditional areas, like credit and market risks, metrics have been refined to a point where most directors feel comfortable that they are getting the right level of information and that management is offering an accurate picture of the firm's risk profile relative to its risk appetite. For non-financial risks, this is much more difficult. A director observed, *"For the more mature risk areas we tend to not be overwhelmed with information. It is the newer areas like reputation risk and operational risks that are not as well established because best practices are not clear and the metrics are not as developed or understood, where we tend to get a lot of information and where it can be difficult to cut it down to a few key metrics."*

One area where boards continue to look for assistance is benchmarking against peers. Several Summit participants encouraged supervisors to provide more feedback: *"That aspect of spreading knowledge across the industry, I think that's where regulators can really help. They do reviews across the industry and we may think we're best in class, but regulators know if we actually are."* While supervisors do this already, one participant encouraged regulators to do more: *"I would push the envelope from a preventative perspective on understanding what people are doing. Are you doing enough cross-institutional testing?"* This feedback can provide the board with a useful outside perspective as they assess management's efforts. One director observed, *"What I think we'll typically find is that we are not as good as we think we are, but we need to be careful that that reaction doesn't cause an unwanted response from management."*

> *"The more expertise you bring in, the clearer it is what you're not good at. You don't want management to stop bringing in experts or stop the flow of information."*
>
> — Participant

Board and risk committee composition remains in flux

A participant noted, *"The composition of the board has changed drastically in recent years. We have added a former military general and an expert on cyber to the board. Every financial institution is trying to bring in new skillsets."* Some boards regularly access external experts – some in the UK have even added outside experts to standing board committees. A participant emphasized, however, that despite having access to more external expertise, a board ultimately retains responsibility for understanding the risks its institution is taking on: *"The board has to get its hands dirty and pick board members willing to do that. Understanding the market and asking experts about what the real deal is. And you need clarity as to what you need on your board—for example, deep technology expertise or someone with more industry knowledge. There is talent out there, but you need to ask the right questions and know what you are looking for."*

Another participant said, *"Another challenge is that the more expertise you bring in, the clearer it is what you're not good at. Then the challenge is encouraging the conversation to talk openly about that. You don't want management to stop bringing in experts or stop the flow of information."*

***

> *"What you realize is that it actually takes a lot of extra hours to become frightened enough about the right things."*
>
> — Participant

Financial institution risk management and oversight will be challenged by a combination of pressure on earnings arising from a difficult macroeconomic environment and non-financial risks that could threaten the resilience of individual institutions and the financial system, yet remain hard to measure and monitor. Directors will therefore need to continue to devote substantial time to understand the evolving risks their institutions face and the steps being taken to manage and mitigate them. A director observed, *"What you realize is that it actually takes a lot of extra hours to become frightened enough about the right things. It's not fewer hours, it's more hours because of these new risk areas and I don't think it can be done in the normal cycle of boardroom sessions."*

Appendix A: Summit Participants

In 2019, Tapestry and EY hosted nine BGLN and IGLN meetings, including the third Financial Services Leadership Summit. In preparation for the summit, Tapestry and EY had more than 40 conversations with directors, executives, regulators, supervisors, policymakers, and other thought leaders. Insights from these discussions helped to shape the summit agenda and inform the enclosed *ViewPoints* documents.

The following individuals participated in discussions for the 2019 Financial Services Leadership Summit:

- Homaira Akbari, Non-Executive Director, Santander
- Bo Brustkern, Co-Founder & CEO, LendIt Fintech
- Martha Cummings, Head of Compliance Strategy & Operations, Wells Fargo
- Sarah Dahlgren, Head, Regulatory Relations, Wells Fargo
- Scott DePasquale, President & CEO, Financial Systemic Analysis & Resilience Center
- Tracy DeWald, Chief Risk Officer, Mutual of Omaha
- Eliza Eubank, Director and Global Head of Environmental and Social Risk Management, Citi
- Robin Finer, Acting Chief Economist and Director of Competition, UK Financial Conduct Authority
- Mike Gibson, Director, Division of Supervision and Regulation, Federal Reserve System
- Sheila Hooda, Nominating and Governance Committee Chair, Prosight Global and Non-Executive Director, Mutual of Omaha
- Brad Hu, Chief Risk Officer, Citigroup
- Adam Hughes, President & Chief Operating Officer, Amount
- Sean Kevelighan, CEO, Insurance Information Institute
- Olivia Kirtley, Non-Executive Director, US Bancorp
- Sara Grootwassink Lewis, Audit Committee Chair, Sun Life
- Alan MacGibbon, Audit Committee Chair, TD Bank
- Stuart Mackintosh, Executive Director, The Group of Thirty
- Trey Maust, CEO, Sheltered Harbor
- Eileen Mercier, Audit Committee Chair, Intact Financial Institution
- Tom Mildenhall, Global Head, Technology Business Development, Bank of America Merrill Lynch
- Scott Moeller, Risk Committee Chair, JPMorgan Securities
- Gerald Murray, Non-Executive Director, USAA

- James Paris, Chief Revenue Officer and Chief Strategy Officer, Avant
- Wayne Peacock, President, Property and Casualty Insurance Group, USAA
- Marty Pfinsgraff, Risk Committee Chair, PNC Bank
- Nathalie Rachou, Risk Committee Chair, Societe Generale
- Peter Raskind, Risk Committee Chair, Capital One
- Ely Ratner, Executive Vice President and Director of Studies, Center for a New American Security
- Bruce Richards, Chair of the Board, Credit Suisse USA
- Jeremy Rudin, Superintendent, Office of the Superintendent of Financial Institutions
- Manolo Sánchez, Former Chair and CEO, BBVA Compass
- Denise Schmedes, Senior Vice President, Supervision Group, Federal Reserve Bank of New York
- Alice Schroeder, Non-Executive Director, Prudential plc
- Alan Smith, Global Head of Risk Strategy, HSBC
- Val Smith, Chief Sustainability Officer, Citigroup
- Doug Steenland, Chair of the Board, AIG
- Thomas Sullivan, Associate Director; Division of Banking Supervision and Regulation, Federal Reserve Board
- Katie Taylor, Chair of the Board, RBC
- Lyndsey Toeppen, Vice President, Insurance, Sandbox Insurtech Ventures
- Cathy Wallace, Chief Risk Officer, State Farm
- Tom Watjen, Non-Executive Director, Prudential plc
- Steve Weber, Professor, School of Information Science, University of California, Berkeley
- Tom Woods, Non-Executive Director, Bank of America
- Juan Zarate, Chair and Co-Founder, Financial Integrity Network; Trustee, Northwestern Mutual

EY

- Andy Baldwin, Global Managing Partner, Client Service
- Jan Bellens, Global Banking and Capital Markets Leader
- Thom Cranley, Americas New England Insurance Advisory Leader
- Peter Davis, Americas Financial Services Advisory Leader
- Seth Flory, Managing Director, Advisory Services
- Gary Hwa, Global Financial Services Markets Executive Chair and Asia-Pacific Financial Services Regional Managing Partner
- John Latham, Financial Services Partner
- Marcel van Loo, EMEIA Financial Services Regional Managing Partner
- Ed Majkowski, EY Americas Insurance Sector and Advisory Leader
- Marc Saidenberg, Financial Services Global Regulatory Network Co-Lead
- Isabelle Santenac, Global Insurance Leader
- Martin Spit, Managing Director, EY-Parthenon

Tapestry Networks

- Dennis Andrade, Partner
- Eric Baldwin, Principal
- Jonathan Day, Vice Chair
- Brennan Kerrigan, Associate
- Tucker Nielsen, Principal
- Marisa Roman, Associate
- Simon Wong, Partner

About this document

About *ViewPoints*

ViewPoints reflects the network's use of a modified version of the Chatham House Rule whereby names of network participants and their corporate or institutional affiliations are a matter of public record, but comments are not attributed to individuals, corporations, or institutions. Network participants' comments appear in italics.

About the Financial Services Leadership Summit (FSLS)

The FSLS is an annual meeting addressing key issues facing leading financial institutions. It brings together non-executive directors, members of senior management, policymakers, supervisors and other key stakeholders committed to outstanding governance and supervision in support of building strong, enduring and trustworthy financial institutions. The FSLS is organized and led by Tapestry Networks, with the support of EY. *ViewPoints* is produced by Tapestry Networks and aims to capture the essence of FSLS discussions and associated research. Those who receive *ViewPoints* are encouraged to share it with others in their own networks. The more board members, members of senior management, advisers and stakeholders who become engaged in this leading-edge dialogue, the more value will be created for all.

About Tapestry Networks

Tapestry Networks is a privately held professional services firm. Its mission is to advance society's ability to govern and lead across the borders of sector, geography, and constituency. To do this, Tapestry forms multi-stakeholder collaborations that embrace the public and private sector, as well as civil society. The participants in these initiatives are leaders drawn from key stakeholder organizations who realize the status quo is neither desirable nor sustainable, and are seeking a goal that transcends their own interests and benefits everyone. Tapestry has used this approach to address critical and complex challenges in corporate governance, financial services, and healthcare.

About EY

EY is a global leader in assurance, tax, transaction, and advisory services to the financial industry. The insights and quality services it delivers help build trust and confidence in the capital markets and in economies the world over. EY develops outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, EY plays a critical role in building a better working world for its people, for its clients and for its communities. EY supports the BGLN as part of its continuing commitment to board effectiveness and good governance in the financial services sector.

Endnotes

[1] Caroline Binham, "UK's Big Banks Told to Publish 'Living Wills' from 2021," *Financial Times,* July 30, 2019.

[2] Lalita Clozel and Liz Hoffman, "Fed Moves to Ease Living Wills, Allowing Large Banks to File Wind-Down Plans Less Frequently," *Wall Street Journal,* April 8, 2019.

[3] International Monetary Fund, *World Economic Outlook: Global Manufacturing Downturn, Rising Trade Barriers* (Washington: International Monetary Fund, 2019), xvi.

[4] Rana Foroohar, "Braced for the Global Downturn," *Financial Times,* August 11, 2019.

[5] "Give Me Some of That: Trump Renews Call for Negative U.S. Interest Rates," *Reuters*, November 12, 2019.

[6] Marcus Ashworth, "Brexit Deal: Here's What Will Happen to U.K. Interest Rates," *Washington Post,* October 17, 2019.

[7] Group of Thirty, *Managing the Next Financial Crisis* (Washington: Group of Thirty, 2018), 8.

[8] Financial Stability Board, *Strengthening Oversight and Regulation of Shadow Banking: A Policy Framework for Strengthening Oversight and Regulation of Shadow Banking Entities* (Basel: Financial Stability Board, 2012), ii.

[9] Jeff Cox, "Shadow Banking Is Now a $52 Trillion Industry, Posing a Big Risk to the Financial System," *CNBC*, April 11, 2019.

[10] Ben S. Bernanke, Timothy F. Geithner, and Henry M. Paulson Jr., "Will We Survive the Next Financial Crisis?" *Politico*, April 16, 2019.

[11] Group of Thirty, *Managing the Next Financial Crisis*, 15.

[12] Wayne Byres, "Reflections on a Changing Landscape" (speech, Risk Management Association Australia CRO Board Dinner, Sydney, August 26, 2019).

[13] Morgan Chalfant, "Deadly Attacks Feared as Hackers Target Industrial Sites," *The Hill*, May 31, 2018.

[14] EY and Institute for International Finance, *An Enduring Course: Surviving and Thriving Through 10 Major Risks Over the Next Decade* (Washington, DC: The Institute of International Finance, November 6, 2019), 25.

[15] Jason Healey, Patricia Mosser, Katheryn Rosen, and Adriana Tache, *The Future of Financial Stability and Cyber Risk*, (Washington, DC: The Brookings Institution, October 10, 2018), 8

[16] Ibid.

[17] Adrian Nish and Saher Naumaan, "The Cyber Threat Landscape: Confronting Challenges to the Financial System," *Carnegie Endowment for International Peace*, March 25, 2019.

[18] Nish and Naumaan, "The Cyber Threat Landscape: Confronting Challenges to the Financial System."

[19] John Graetz, Walter Hoogmoed, Alfred Spahitz and Christopher Spoth, "Managing Vendor Risk: The Lines of Defense for Banks," *The Wall Street Journal,* May 31, 2013.

[20] Dr. Michelle Tuveson and Simon Ruffle, "Diversity is the Way to Avoid Cyber Collapse," *Financial Times*. April 26, 2014.

[21] Healey, Mosser, Rosen and Tache, "The Future of Financial Stability and Cyber Risk."

[22] Canalys, Cloud market share Q4 2018 and full year 2018. February 2019.

[23] Financial Services Information Sharing and Analysis Center. "FS-ISAC Announces the Formation of the Financial Systemic Analysis & Resilience Center (FSARC)," news release, accessed December 2, 2019.

[24] Leika Kihara, "IMF's Lagarde Highlights Potential Disruptive Nature of Fintech," *Reuters*, June 7, 2019.

[25] Kihara, "IMF's Lagarde Highlights Potential Disruptive Nature of Fintech," *Reuters*, June 7, 2019.

[26] The Libra Association, *Libra White Paper* (Geneva, Switzerland: The Libra Association, accessed September 2, 2019), 1.

[27] Casey Newton, "Read the Full Transcript of Mark Zuckerberg's Leaked Internal Facebook Meetings," *The Verge*, October 1, 2019.

[28] Peter Rudegeair and Liz Hoffman, "Next in Google's Quest for Consumer Dominance: Banking," *Wall Street Journal,* November 13, 2019.

[29] Martin Sandbu, "How Facebook's Libra Fuelled Push for Central Bank-Run Digital Currencies," *Financial Times*, September 23, 2019.

[30] Mark Carney, "The Growing Challenges for Monetary Policy in the Current International Monetary and Financial System" (speech, Jackson Hole Symposium 2019, Wyoming, USA, August 23, 2019).

[31] Kate Rooney, "As Facebook's Libra Faces Headwinds, China is Racing to Launch Its Own Global Cryptocurrency," CNBC.com, October 15, 2019.

[32] Rooney, "As Facebook's Libra Faces Headwinds, China is Racing to Launch its Own Global Cryptocurrency," CNBC.com, October 15, 2019.

[33] Patrick Cleary, William Harding, Jeremy McDaniels, Jean-Philippe Svoronos and Jeffery Yong, *Turning up the Heat—Climate Risk Assessment in the Insurance Sector, FSI Insights on Policy Implementation No. 20* (Basel, Switzerland: Bank for International Settlements, November, 2019), 1.

[34] Margherita Giuzio, Dejan Krusec, Anouk Levels, Ana Sofia Melo, Katri Mikkonen, and Petya Radulova, *Climate Change and Financial Stability* (Frankfurt, Germany: European Central Bank, May 2019).

[35] Jim Dobson, "Shocking New Maps Show How Sea Level Rise Will Destroy Coastal Cities By 2050," Forbes, October 30, 2019.

[36] Jamie Powell, "Climate Change: The CMBS Angle," Financial Times, October 28, 2019.

[37] William Wilkes, "Insurers Worry a Financial Crisis May Come from Climate Risks," Bloomberg, February 22, 2019.

[38] Network For Greening The Financial System, *A Call for Action: Climate Change as a Source of Financial Risk* (Paris: NGFS Secretariat/Banque De France, April 2019), 17.

[39] Network For Greening The Financial System, *A Call for Action: Climate Change as a Source of Financial Risk,* 13.

[40] Sarah Breeden, "Avoiding the Storm: Climate Change and the Financial System" (speech, Official Monetary and Financial Institutions Forum, London, April 15, 2019).

[41] Thomas Cranley, Jeremy Weiss, and Jeff Wenger, *NextWave Insurance: Personal Lines and Small Commercial— How Insurers Must Change in a Fast-Moving World* (New York: Ernst & Young LLP, 2019), 11.

[42] Glenn D. Rudebusch, *Climate Change and the Federal Reserve*, FRBSF Economic Letter (San Francisco, CA: Federal Reserve Bank of San Francisco, March 25, 2019), 3.

[43] Irina Ivanova, "Climate Change Could End Mortgages as we Know Them", CBS, November 8, 2019.

[44] Cleary, Harding, McDaniels, Svoronos and Yong, Turning up the Heat –Climate Risk Assessment in the Insurance Sector, 3.

[45] Becca Habegger, "Insurance Commissioner 'Hopeful' He Can Help Homeowners Losing Coverage," ABC10, August 23, 2019.

[46] Task Force on Climate-Related Financial Disclosures, *Recommendations of the Task Force on Climate-Related Financial Disclosures* (TCFD, June 2017), v.

[47] Financial Stability Board, "TCFD Report Finds Encouraging Progress on Climate-Related Financial Disclosure, but Also Need for Further Progress to Consider Financial Risks," news release, June 5, 2019.

[48] Giuzio, Krusec, Levels, Melo, Mikkonen and Radulova, "Climate Change and Financial Stability."

[49] Christopher Cundy, Adam Leach, and Ronan McCaughey, "Climate Change Can't be Captured in Solvency II Capital, Says Eiopa," InsuranceERM, June 3, 2019.

[50] Caroline Binham and David Crow, "Carney Plans to Test UK Banks' Resilience to Climate Change," Financial Times, December 17, 2018.

[51] "Climate Change Ranked as Top Emerging Risk," *InsuranceERM*, 23 October 2019.

[52] UNEP Finance Initiative, "Principles for Sustainable Insurance," accessed September 18, 2019; UNEP Finance Initiative, "Principles for Responsible Banking," accessed September 18, 2019.

[53] UNEP Finance Initiative, "Principles for Sustainable Insurance: Signatory Companies," accessed September 18, 2019. UNEP Finance Initiative "Principles for Responsible Banking: Signatories," accessed September 18, 2019.

[54] Carmen Reinicke, "An Alliance of Major Investors Overseeing $2.4 Trillion Has Committed to Making Portfolios Entirely Carbon-Neutral by 2050," *Markets Insider*, September 23, 2019.

[55] Sarfaz Thind, "Fossil fuel exclusion proves a slow burn for US insurers," Insurance Asset Risk, October 3, 2019.

[56] IIF/EY, *An endurance course: surviving and thriving through 10 major risks over the next decade*, (November 6, 2019), 25.

[57] Dave Chaffey, "Global social media research summary 2019," Smart Insights, February 12, 2019