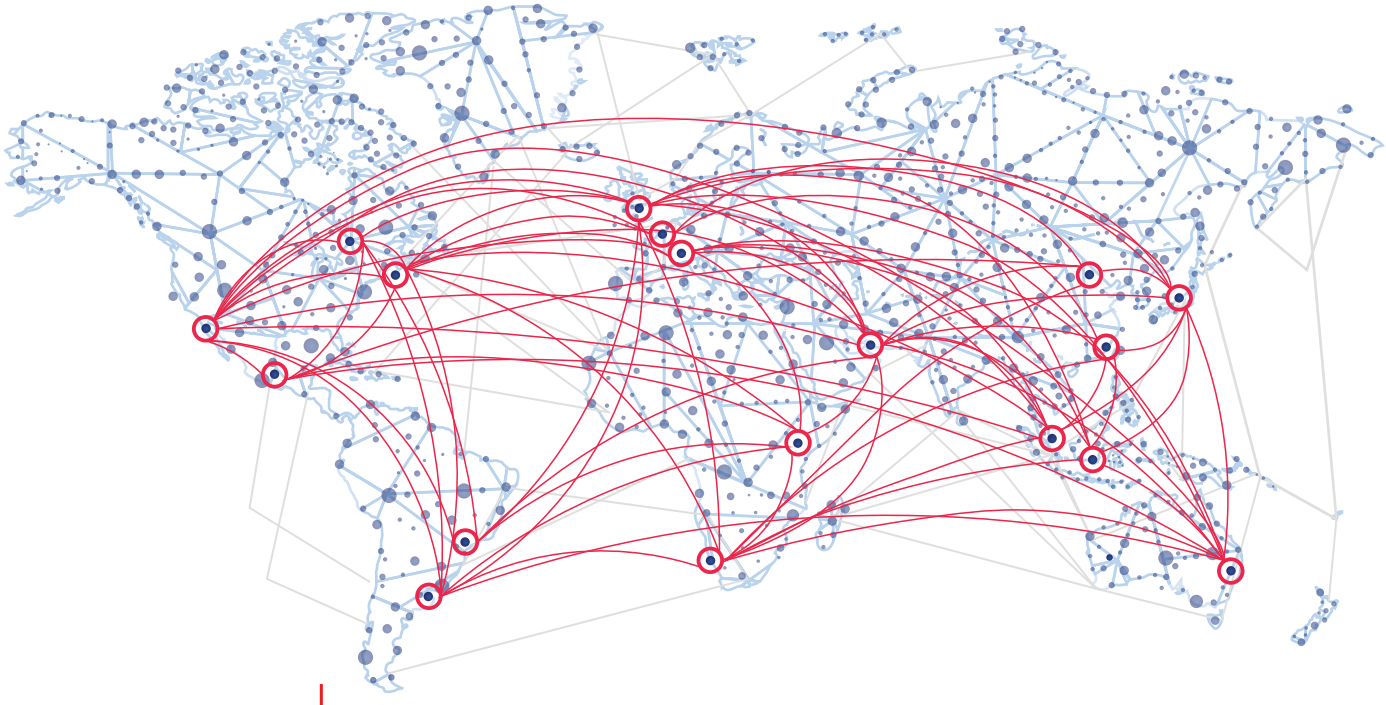
SwissFinanceCouncil
Fostering International Dialogue

GLOBAL SYSTEMIC STABILITY AND EVOLVING RISKS



Global Systemic Stability and Evolving Risks

With special thanks to our external contributors:
Dominique Laboureix and Prof. Sadie Creese.

FOREWORD

The regulatory environment in which the financial sector operates has evolved significantly since the financial crisis of 2008. New frameworks have been introduced with the aim of enhancing the overall financial system's resilience. Numerous new regulations and stepped-up international cooperation over the last ten years have led to much-improved capital buffers, better liquidity planning, enhanced resolvability as well as better overall management of risk. At the same time, diverging national implementation of globally agreed regulation accelerates regulatory fragmentation, leading to overlapping and incompatible rules and hence significantly increased complexity and risk of regulatory arbitrage in the financial system which is further underscored by a lack of effective cooperation between regulators in different jurisdictions (this was the key theme of last year's Discussion Paper of the Swiss Finance Council titled 'International Regulatory Cooperation to counter the Risks of Fragmentation'). Such undue discretion for national regulators can only lead to market fragmentation which ultimately distorts competition and has a noticeable impact on cross-border investment, growth and job creation within the EU Single Market and beyond. We hence welcome that the Financial Stability Board as well as the Japanese G20 Presidency have identified regulatory fragmentation as a key challenge to be addressed.

This year's Swiss Finance Council Discussion Paper examines the extent to which the financial system has stabilised through new regulatory frameworks and, at the same time, asks what evolving risks are likely to gain prominence over time. Among evolving risks, we have identified three key areas which we explore in the form of case studies:
(i) the cumulative risks from complex and multi-level regulation; (ii) cybersecurity and operational resilience overall; (iii) and the risks associated with climate change. While there is a strong dialogue between the financial sector and the regulatory community concerning these risks, we feel that their increased prominence over the last few years necessitates a new engagement model. These risks could threaten global systemic financial stability if they are not adequately addressed by both the public as well as the private sector. Concrete and joint action towards a more robust system as well as designing and implementing procedures for use in potential future crises is now key.

We strongly believe in an open dialogue between policymakers and the financial sector. Establishing principle-based global regulatory coordination should be at the core of policy objectives. And we will need to keep in mind the global dimension of financial markets, in particular of the evolving risks we identified, seeking regulatory alignment with the EU's main trading partners and significant financial centres.

Drawing on the Discussion Paper's case studies, as well as on our analysis of the global regulatory reforms accomplished to date, we propose three sets of recommendations that could serve as building blocks for both regulators and the financial industry to address and manage evolving risks in a way that maintains global systemic stability:
(i) achieve completion of prudential reforms, assess their impact and develop a forward-looking approach for the future; (ii) deliver financial stability in an efficient manner; and (iii) move to a new engagement model to prepare for evolving risks. We trust that you will find the publication a thought-provoking contribution to this important debate.

Urs Rohner
Chairman of the Board
Credit Suisse Group

Axel A. Weber
Chairman of the Board
UBS Group

Lukas Gähwiler
Chairman of the Board
UBS Switzerland

CHAPTER 1

GLOBAL SYSTEMIC STABILITY AND EVOLVING RISKS

Introduction

The global financial system has changed dramatically since the financial crisis in 2008. The crisis had various causes such as excessive real estate indebtedness in the USA in particular, flawed corporate governance and consumer protection frameworks as well as high-risk financial instruments which eventually led to the 2008 financial crisis.

In response, central banks, regulators and policymakers introduced new requirements aiming to increase the stability of the system.

Large banks have significantly improved their capital ratios compared to pre-crisis levels and are subject to recovery and resolution plans to allow authorities to take early coordinated action or to ensure an orderly process in the event of failure. They have also strengthened their corporate governance and organisational cultures. These combined efforts result in a situation where banks are in much better shape today and contribute to a safer financial system, especially during episodes of stress. Consequently, the industry expects the wave of new regulatory requirements to gradually ebb away over the coming years – a view shared by global policymakers and regulators.

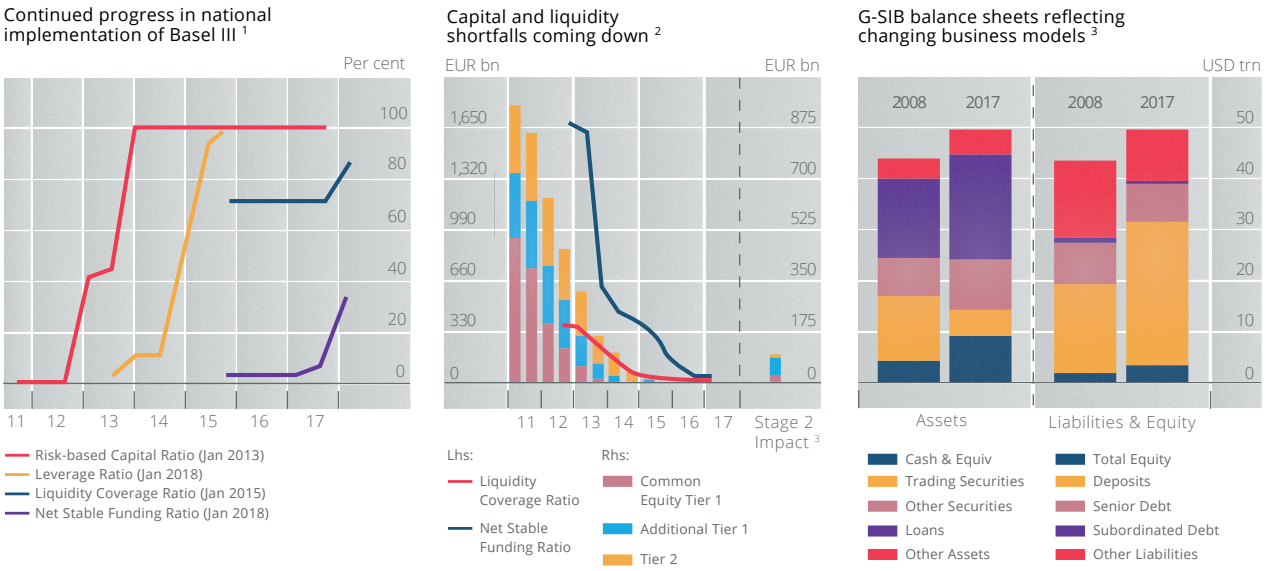
The 2018 Annual Economic Report of the Bank for International Settlements (BIS) confirms that the impact of reform is already evident. Trends in aggregate Global Systemically Important Bank (G-SIB) balance sheets, for example, tally quite closely with the reform's objectives. More and higher-quality capital, less reliance on short-term wholesale funding, larger High-Quality Liquid Asset (HQLA) buffers and a shift away from business lines such as proprietary trading (apparent from the shedding of trading assets) are the consequence.[1]

The chart below demonstrates that good progress has been made in national implementation of Basel III and how regulatory changes have impacted banks' balance sheets and thus contributed to a more resilient financial system.

There are though signs that previous risks might re-enter the system and we see the emergence of risks in new spheres. Global debt ratios have continued to grow significantly. From 2008 to mid-2017, global public debt more than doubled, reaching USD 60 trillion (Figure 2) and exceeding annual GDP in Japan, Greece, Italy, Portugal, Belgium, France, Spain, and the United Kingdom among others.[2]

Even though the financial system might have become less vulnerable, debt shift towards the public sector must be carefully considered by policymakers and government in order to prevent another crisis.

Figure 1: Implementation of new requirements and banks' adjustments

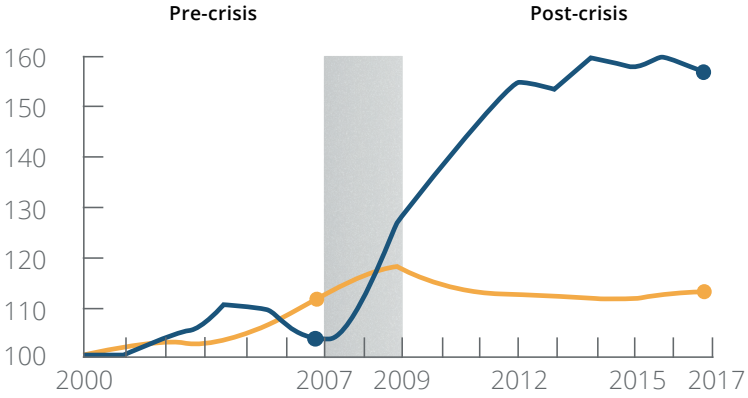


[1] Percentage of BCBS member jurisdictions in which each standard is in force; agreed implementation dates in parentheses. [2] The height of each bar shows the aggregated capital shortfall considering requirements for each tier (i.e. CET1, Additional Tier 1 and Tier 2) of capital for the major internationally active banks monitored by the BCBS (BCBS (2018)). [3] Total values; based on a balanced sample of 28 G-SIBs. Cash & equiv = cash and cash equivalents.

Sources: BCBS; BCBS, Basel III monitoring report, December 2017 and March 2018; SNL; BIS calculations.

Figure 2: Public debt increased rapidly after the crisis in advanced economies

Debt by sector in advanced economies[1]
% of GDP (Index: 2000 = 100)



Actual debt-to-GDP ratio %

Year	2000	2007	2017
Public	67 (index:100)	69 (index:103)	104 (index:157)
Private	144 (index:100)	164 (index:114)	164 (index:114)

Change in debt-to-GDP ratio[2]
Percentage points

	2000-07	2007-H1 2017
Public	+2	+35
Private	+20	0

1 Australia, Austria, Belgium, Canada, Denmark, Finland, France, Germany, Greece, Hong Kong, Ireland, Israel, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Portugal, Singapore, South Korea, Spain, Sweden, Switzerland, the United Kingdom and the United States

2 Includes household and non-financial corporate sector debt

NOTE: Debt as percent of GDP is indexed to 100 in 2000; numbers here are not actual figures

SOURCE: BIS; McKinsey Country Debt Database; McKinsey Global Institute Analysis

Low interest rate policies furthermore mean that financial institutions have become less profitable. In addition, banks have decreased their international business activities, having sold more than USD 2 trillion of assets globally since the crisis.[3]

Below we provide key examples of past regulatory reforms that have contributed to a more resilient financial system. These examples are also important drivers for the new risk management practices that the industry has put in place.

We will argue that the agreed reforms will only deliver their full benefits if implemented consistently without fragmentation and national ring fencing; also, if some associated operational issues are addressed. We also acknowledge that risks which are not rooted in the banking system are emerging and need to be addressed by regulators. In this paper we look at three types of such risks that have potentially a significant impact on financial stability and have increasingly gained in intensity over the last years: regulatory complexity, cybersecurity and climate change. Among the available tools, we would highlight the use of new technology which can help in identifying and addressing these risks. RegTech, as it is called, should be actively supported by the regulatory and supervisory practices. Furthermore, there are a number of adverse consequences which will surface over the coming years and which need to be addressed by regulators and politicians appropriately based on an open and fact-based debate among all relevant stakeholders, including the industry.[4]

Key examples of accomplished global reforms

The Basel III framework

Basel III was one of the main responses to the financial crisis addressing shortcomings of the pre-crisis regulatory framework. The comprehensive reform of the prudential framework for banks focused on increasing the quantity and quality of required regulatory capital, a new approach to market risk and counterparty credit risk, the introduction of macro-prudential capital buffers, additional capital buffers for G-SIBs, a leverage ratio and a Liquidity Coverage Ratio (LCR) as well as a Net Stable Funding Ratio (NSFR). Furthermore, in order to promote simplicity, comparability and less variability related to internal models and to restore the credibility in the calculation of Risk-Weighted Assets (RWA) the Basel Committee adopted the following changes by end 2017:

- Enhancing the robustness and risk sensitivity of the standardised approaches to credit and operational risk, in order to facilitate the comparability of banks' capital ratios;
- Constraining the use of internally modelled approaches, by placing limits on certain inputs used to calculate RWA under the Internal Ratings-Based (IRB) approach to credit risk and by removing the use of the modelled approach to operational risk;

- Finalising the leverage ratio, which now includes a buffer to further limit the leverage of G-SIBs; and

- Replacing the existing Basel I-based floor with a robust aggregate 72.5% output floor based on the Committee's revised standardised approaches.[5]

The reforms have considerably strengthened the banking system. Since 2011, the Tier 1 leverage ratio of major internationally active banks has increased by over 65% (from 3.5% to 5.8%), while their Common Equity Tier 1 (CET1) risk-weighted ratio has increased by over 70% (from 7.2% to 12.3%). The bulk of this change was achieved by an increase in banks' CET1 capital resources (from EUR 2.1 trillion to EUR 3.7 trillion). There has also been a corresponding reinforcement of banks' liquidity: holdings of liquid assets have increased by 30% (from EUR 9.2 trillion to EUR 11.6 trillion).[6]

Market regulation of derivatives

'The opacity of the underlying exposures, together with questions about counterparty credit worthiness and the inherent leverage of OTC derivatives had been a major factor for the collapse of Lehman.' [7]
The financial crisis underscored the importance of central clearing to reduce systemic risk. In reaction, G20 leaders decided at the 2009 Pittsburgh Summit that all standardised Over-the-Counter (OTC) derivative contracts should be traded on exchanges or electronic trading platforms, where appropriate, and cleared through central counterparties (CCPs), by end 2012 at the latest; that OTC derivative contracts should be reported to trade repositories; and that Non-centrally cleared contracts should be subject to higher capital requirements.[8]

Consequently, the new central clearing and reporting requirements on derivatives transactions lead to netting opportunities to reduce risks, increased transparency and better risk management overall.

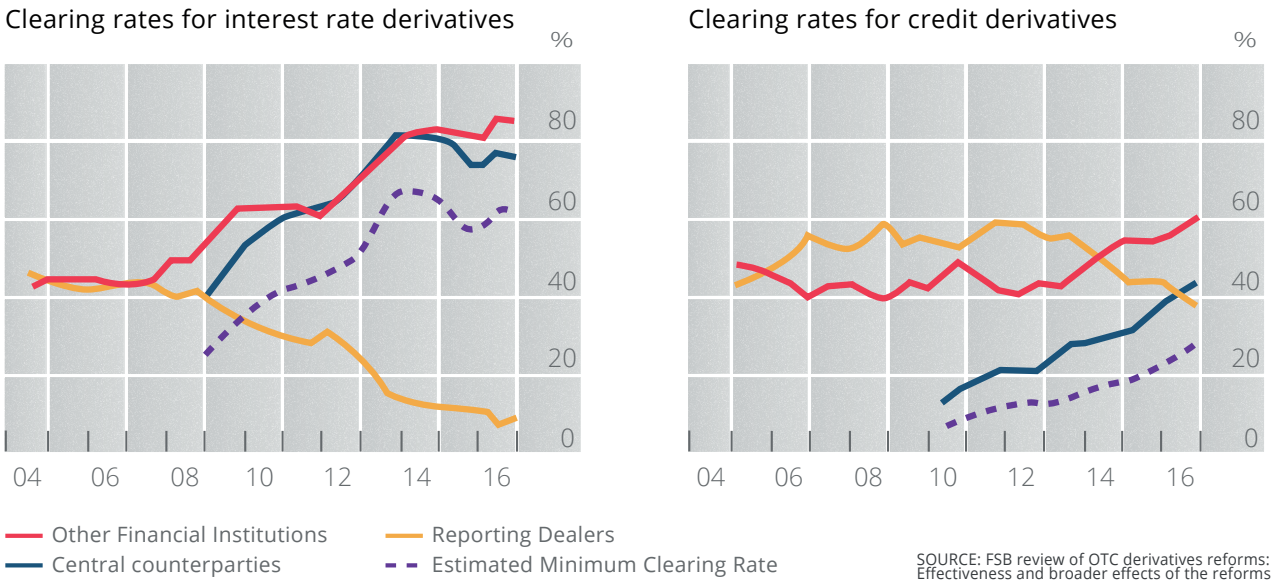
Central clearing is now a key feature of global derivatives markets. Almost 80% of OTC interest rate derivative contracts are now cleared via central counterparties - up from around 40% in 2009. The share of central clearing has also grown in other product markets, such as credit derivatives. The increasing use of CCPs meets the aim of post-crisis reform policy.

The graph below demonstrates that the 2009 policy recommendations were swiftly implemented by the industry.

Addressing too-big-to-fail

Ten years ago, Lehman Brothers Holdings Inc. failed. The financial crisis demonstrated that large financial institutions could not be resolved in a manner that maintained the continuity of critical functions and without exposing taxpayers to the risk of loss. The largest financial institutions were therefore considered to be *'too-big-to-fail'* (TBTF).[9]

Figure 3: Notional amounts outstanding by counterparty type, in percent



SOURCE: FSB review of OTC derivatives reforms: Effectiveness and broader effects of the reforms

Decisive actions have been taken to address the moral hazard that, as argued by policymakers, was posed by G-SIBs being 'too-big-to-fail' and the resulting loss in market discipline. The framework adopted is a multifaceted set of measures, the core of which is bail-in and the Total Loss Absorbing Capital (TLAC) concept with gone-concept capital, intended to absorb losses after an institution has failed and to facilitate an orderly resolution as well as the recapitalisation of continuing critical functions. Taken broadly, this fundamental reform includes:

- Requirements for additional loss absorption capacity for G-SIBs;
- G-SIBs undergoing more intensive and intrusive supervision with higher expectations, including for risk governance, internal control and risk data aggregation capabilities;
- International supervisory colleges being put in place for better coordination between home and host authorities in assessing risks facing G-SIBs;
- The development of an international standard laying out the responsibilities, instruments and powers that national resolution regimes should introduce into national law (the Financial Stability Board's 'Key Attributes of Effective Resolution Regimes for Financial Institutions').

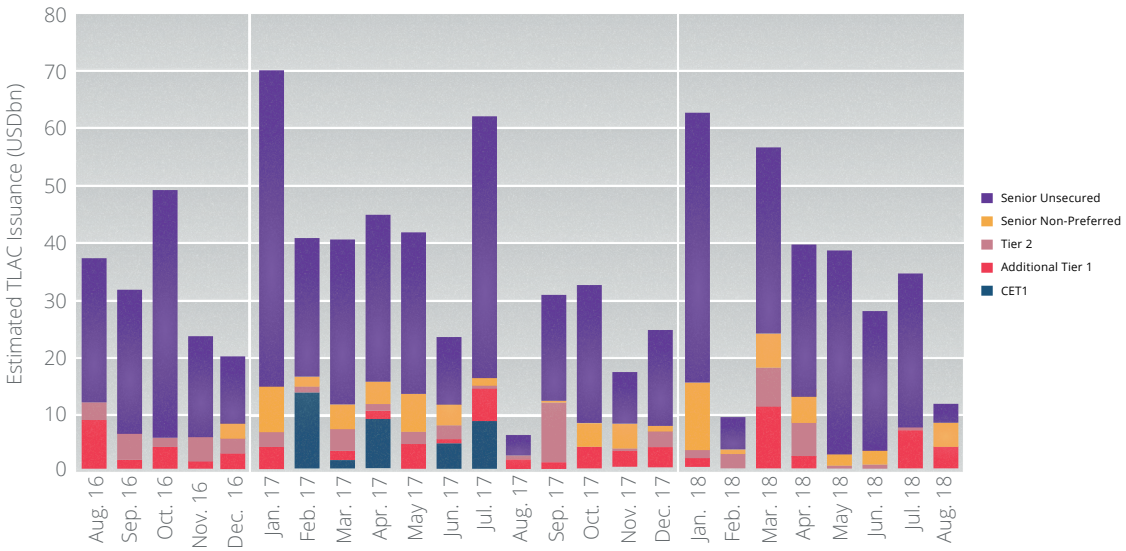
'Many G-SIBs are estimated to already meet, or be close to meeting, the 2019 minimum external TLAC requirement, while a subset of those G-SIBs is also estimated to be well placed against the 2022 minimum external TLAC requirement.' [10]

Corporate and risk governance

In 2009, the Organisation for Economic Cooperation and Development looked into what went wrong in corporate governance arriving at a severe assessment: *'When corporate governance arrangements were put to a test, corporate governance routines did not serve their purpose to safeguard against excessive risk taking in a number of financial services companies. A number of weaknesses have been apparent. The risk management systems have failed in many cases due to corporate governance procedures rather than the inadequacy of computer models alone: information about exposures in a number of cases did not reach the board and even senior levels of management, while risk management was often activity rather than enterprise-based. These are board responsibilities. In other cases, boards had approved strategy but then did not establish suitable metrics to monitor its implementation. Company disclosures about foreseeable risk factors and about the systems in place for monitoring and managing risk have also left a lot to be desired even though this is a key element of the Principles.'* [11]

Policymakers reacted swiftly and pushed for strengthened good governance principles which resulted in a new governance culture marked by the following significant changes:

Figure 4: Estimated G-SIB issuance by eligible TLAC instrument (August 2016-August 2018)



Sources: Bloomberg, FSB secretariat estimates

The chart above demonstrates that during 2017 and 2018 banks have continued issuing substantial amounts of external TLAC.

- Banks recognise the critical role of boards and the need to strengthen their governance of risk. This includes greater involvement in evaluating and promoting a strong risk culture in the organisation; the establishment of an organisation's risk appetite; the oversight of management's implementation of the agreed risk appetite and alongside the overall governance framework.
- The role of senior management, including the Chief Risk Officer (CRO) has been shaped to the new environment. The CRO's independence and his or her access to the board has been upgraded accordingly.
- A June 2018 report of the Basel Committee for Banking Supervision (BCBS) confirms progress made in implementing the principles surrounding risk data aggregation. According to this report, sophistication of banks' risk management and internal control infrastructure is keeping pace with changes to their risk profile in the external risk landscape.[12]
- In order to improve the incentive structure, the Financial Stability Board (FSB) has introduced standards on sound compensation practices. Compensation tools, together with other measures, can play an important role in addressing misconduct risk by providing both ex ante incentives for good conduct and ex ante adjustments that ensure appropriate accountability. Since the issuance of the FSB Principles and Standards in 2009, supervisors and firms have directed attention to improving the link between risk governance and compensation practices. This has better aligned compensation with sound risk-taking behaviour with a view to the long-term health of financial institutions.[13]
- Technological transformation and availability of data are increasingly used to strengthen risk management practices.

What remains to be done?

In the following we point to two key factors that must be considered in order to make the reforms most effective.

We also look at some risks outside the prudential area that should be addressed by smart regulation. Evolving risks emerge continually and should not be left unaddressed. For instance, climate change risk and cybersecurity considerations have gained importance in recent times and smart regulation must follow these developments. We also identify increasing regulatory complexity as an evolving risk.

Avoiding inconsistent implementation and fragmentation

At the 2009 Pittsburgh Summit, the G20 called on policymakers to *'take action at the national and international level to raise standards together so that our national authorities implement global standards consistently in a way that ensures a level playing field and avoids fragmentation of markets, protectionism, and regulatory arbitrage.'* [14] Global coordination and consistent implementation have been a long-standing objective of the international community.

All financial reform initiatives that followed the Pittsburgh Summit contributed to building a significantly more resilient financial system. However, recent developments point at increasing cases of national divergence from international standards, or even new rules introduced by national authorities motivated by a narrower perspective on financial stability, either to protect their domestic markets or because of conceptual differences or misalignment with internationally agreed standards. Such approaches create inconsistencies that can put at risk efforts to build a stronger financial system. Liquidity can be trapped, funding unavailable, compliance made more complex and inefficient for firms, but also challenging to supervise for national authorities. The capacity and benefits global banks can bring to global customers are affected with immediate implications for economic growth and financial stability.

Consistent implementation of internationally agreed frameworks is key. Otherwise, fragmentation in regulation and supervisory practices can lead to:

- Making global operations a true challenge for global banks as they must comply with multiple national regimes. Inefficient allocation of capital and resources and high compliance costs will be the consequence. This poses level playing field questions and opens the door to regulatory arbitrage.
- Complicating the design and implementation of group-wide IT solutions for risk management purposes.
- Distrust among national supervisors resulting in further national ring-fencing and thus undermining the purpose and efficiency of global standards.

Fragmentation along national lines is a challenge to global financial stability. *'Fragmentation can impair financial stability by reducing market liquidity and trapping scarce sources. It can drag efficiency and economic growth. Combatting market fragmentation should be our common goal'.*[15] Fighting fragmentation of financial markets is one of the priorities of the Japanese 2019 G20 Presidency.

Operational issues

Efficient risk management requires a sound regulatory basis as well as banks to be sufficiently profitable (the first buffer against losses before capital). Against this background we see the following challenges:

- National rules that require inflexible and high levels of pre-positioned internal loss absorption (internal TLAC) in individual legal entities without the ability to deploy these resources in other legal entities when financial group support would be needed. This approach contradicts the philosophy of a Single Point of Entry resolution strategy and can increase financial stability risks. A working paper by Ervin Wilson demonstrates that if such ring-fencing becomes pervasive, the likelihood of failure can increase by 5x or even 15x compared to an Integrated Bank where internal capital is fully mobile.[16]
- Funding in resolution is key to maintaining the critical functions of a bank throughout the resolution process until the institution is resolved and the remaining part stabilised. Currently no adequate framework exists at European level, which constrains the application of optimal bank resolution. A worry also expressed by the Chairwoman of the Single Resolution Board: *'While private measures are expected to narrow gaps, the impact must be seen against the backdrop of potential sizes of liquidity needs. Looking at historic cases, support to individual banks in stress easily count triple billion figures. Precisely for this reason, FSB guidance recommends establishing temporary public backstop funding mechanisms. Such a tool currently does not exist in the Banking Union, which is a missing piece in the overall framework.'* [17]
- Bail in execution, where additional clarity is needed to facilitate the operational execution of bail-in while maintaining financial stability. Valuation issues, operational continuity and disclosure are additional issues authorities and firms will need to continue working on. This can provide even more assurance concerning the financial system's strength and its readiness to face a new crisis.

Regulatory complexity

While we acknowledge that financial innovation, and the global scale of financial markets, requires new and more complex rules, we caution against a framework that is too complex to be assessed and consistently applied and too expensive to comply with:

- It is becoming more difficult to meet the requirements imposed by overlapping regulation. New policy issues are being added to the regulatory agenda in the field of Environment, Social and Governance (ESG). Legal and compliance costs have increased significantly over the last decade; our first case study shows that banks' analysts estimate these to account for 7% - 9% of total operating expenditure.
- Group management is becoming more demanding when an activity is subject to multiple control mechanisms (e.g. risk-based capital, input & output floors, leverage ratio and stress tests / Pillar 2 requirements) that may also differ according to the jurisdictions where legal entities of the group are based.
- Investors will find it more difficult to extract and verify necessary information and to make a well-informed decision. If complexity and information asymmetry (only the most sophisticated investors will be able to extract, analyse and compare relevant information) impede market transparency, then price formation as regards banks' equity and debt capital instruments is challenged. The same applies to information about potential losses incurred by investors in case of bank resolution. Ultimately market discipline will be eroded, and less sophisticated investors will have an information disadvantage compared with more sophisticated ones.

Market fragmentation and regulatory complexity are also addressed as an evolving risk by the FSB. In a recent speech, FSB Chair Randal K Quarles stated that it is important to have a strong level of financial resilience with reforms that are more efficient, simple, transparent and tailored.[18] For 2019, the recent FSB work programme includes a report on market fragmentation and the identification of tools that national authorities can use to address the risk of market fragmentation arising from regulatory or other causes.[19]

Regulation and supervisory practices can support banks in their efforts to drive innovation and encourage new technology-based solutions to facilitate compliance of regulatory requirements. Supervisors are beginning to recognise benefits new technology can deliver by acknowledging that *'Over time, we can become more efficient in the way that data is shared between banks and supervisors. We are aware that the bespoke data requests we make to banks can generate a substantial burden. With collaboration between the industry and supervisors, it could be possible to improve our data-sharing systems via automation. This could make data provision increasingly timely and accurate for us supervisors, whilst at the same time making things increasingly painless for bankers.'* [20]

Cybersecurity

Risks associated with new technologies have not come as a surprise. They are receiving increasing attention from both regulators and financial institutions because of their magnitude, interconnectedness with other industries and the many challenges they pose to the functioning of society in general and of the economy in particular. According to the World Economic Forum (WEF), cyber-attacks are seen as the biggest threat to doing business across Europe.[21] Some even fear that cyber-attacks could trigger the next financial crisis if cyber-risks are not addressed properly.[22] For the Bank of England and the Financial Conduct Authority (FCA), firms should assume that fraud, data breaches and business disruption will occur, and they should think how they can continue offering critical services in such situations.[23]

The focus has shifted from setting up principles and designing systems to real implementation and testing with the aim of ensuring cyber-resilience and ultimately systemic stability. Central banks, including the European Central Bank, have done substantial work in this respect. Cyber-threats and attacks require institutions to permanently reassess and adapt to the evolving environment. Not only must senior management pay attention to cybersecurity, but cybersecurity must be driven at Board level and be integrated into firms' business strategy and risk management, as we explain in our second case study. The security of assets and identity has indeed become ever more critical in the digitalised environment in which financial institutions evolve. If not addressed properly and urgently, risks associated with the unprecedented level of technological innovation might simply prevent the same digital innovation from fostering economic growth, creating new jobs, contributing to the monitoring of more traditional risks (see below) and, more generally but equally important, to generating the necessary trust between consumers and providers of financial services and among regulators and supervisors.

The challenges posed by cyber-risks are inherently global and cross-border in nature. The financial system has made progress in identifying issues and implementing measures to tackle cyber-risks. As we demonstrate in our second case study, there is a solid framework for supranational governance of cybersecurity. This will need to be further aligned and simplified as the characteristics and concentration of risk scenarios evolve and cyber-attacks increase in both magnitude and complexity. This in turn requires still stronger cooperation between the private and public sectors and an international alignment of cybersecurity regulation and practices. A fragmented regulatory landscape will only serve those who deliberately want to disrupt the functioning of financial markets as cyber-attackers will always look for the weakest link. We therefore need consistent rules and requirements for similar activities regardless of the legal form a firm is organised in, or how large or small it is.

The public and private sectors should work together, across borders, to share information about attacks, exchange best practices, and continually improve security systems to deter cyber-criminals. Existing barriers to effective information sharing should be addressed, primarily through reinforcing cross-border coordination of the various actors. Regulators should coordinate national frameworks, enabling the cross-border sharing of information about cybersecurity incidents. Finally, cybersecurity must be addressed in an ecosystem perspective, i.e. going beyond the financial sector to also include communication, energy and transport sectors for instance. Last but not least, we should increase digital and financial literacy to enable consumers to operate both efficiently and safely in the digital environment.

Climate change risks

Climate change does not constitute a new risk category. Floods and other environmental risks can have repercussion for credit or operational risk and have been addressed from a risk management and disclosure perspective. Including those parameters in models is essential to take into account what should no longer be considered remote or theoretical scenarios, but rather elements that can influence the resilience of firms.

In turn, by considering these new parameters, the pricing of products and reallocation of assets can have a notable influence on reversing the trend towards resource depletion and its economic, financial and social stability implications. Realigning financial flows towards a low-carbon economy is not something that purely has to be brought about by setting strict regulatory boundaries and prescriptive rules. On the contrary, there is a market that shows great potential for innovation – in particular if it can be further unlocked by removing existing regulatory hurdles.

Regulation should therefore play a role. Elaborated in a constructive dialogue with the industry, its impact can be significant. A better supported taxonomy for sustainable products would be useful for investors to better understand the sustainable finance landscape. The European Commission's efforts to develop a broadly supported taxonomy for sustainable products might be a good starting point if its design is flexible enough to be adopted globally without hindering market access or innovation in the area of sustainable finance.

BOX

*Statement by **Dominique Laboureix**, Member of the Board, Single Resolution Board*

What has been achieved since the crisis?

In the crisis, regulators did not have the tools necessary to address bank failures. Since then, European legislators and global standard-setters have made significant changes to ensure that banks could be resolved without use of public funds. The Financial Stability Board agreed both the Key Attributes for effective resolution regimes and the Total Loss Absorbing Capacity termsheet, setting international principles for managing bank failures.

European legislators both implemented a resolution framework across the EU (the Bank Recovery and Resolution Directive) and built a single mechanism to manage bank failure at the level of the Banking Union with the Single Resolution Mechanism Regulation. While the international standards were designed for G-SIBs, the European framework is applicable to all banks in the EU. The Single Resolution Board (SRB) was set up in 2015 to create a single European authority responsible for preparing resolution plans and, if necessary, deciding on resolution schemes for significant banks, as well as other cross-border groups. This provides for integrated decision-making across the 19 different Member States of the Banking Union.

In the SRB's first resolution case on 7 June 2017, of Banco Popular Español, the critical functions of Banco Popular were protected, and adverse effects on financial stability and the real economy avoided, without using any public funds. This showed that the new regime can work – but of course, there is always room for fine-tuning.

Indeed, the work of resolution is moving from the policy-based to the practical. The SRB is adopting resolution plans, with a defined strategy and preferred tools, for all the banks under its remit. The SRB also works on Minimum Requirement for own funds and Eligible Liabilities (MREL) and has now published its policy for both the first wave of resolution plans (mainly for banks that previously did not have binding MREL targets), and also for the second wave (the most complex banks with Resolution Colleges). These requirements are set in the context of the currently applicable legal framework, but we expect that these requirements will ensure banks are better placed to meet the future requirements.

In the EU, legislators have agreed to refine the framework for resolution, and the legislative process for this refinement is now reaching a conclusion. Once the new legislative framework comes into force, it will be for the SRB to implement it from a practical perspective.

Evolving risks

The finance world is ever-evolving, and so too are the challenges. An important challenge identified by the SRB is the complexity and interactions of the different frameworks, in particular the link between the insolvency and resolution systems. Only action by Member States to harmonise insolvency laws will address this issue.

There is also the broader challenge of maintaining international cooperation on resolution, which is critical for the resolution of global banks.

Beyond the banking sector, other actors also affect financial stability. Among them, CCPs have become even more important since the financial crisis. The SRB has an interest in the development of an effective CCP resolution framework because many of the banks under its remit are clearing members of these CCPs and are therefore exposed to their tail-risk. We welcome the ongoing work of the Commission in this area.

Beyond CCPs, there are other actors, including unregulated counterparts and insurance firms, which should also be considered. It is important for the authorities to monitor developments in the financial system and react appropriately.

Another important risk is Brexit. To ensure that this does not undermine the SRB's work, banks must plan for any possible outcome in the ongoing negotiations. The SRB is closely monitoring these plans. In terms of the SRB approach, we have now published our expectations. Of course, we expect that all banks must be resolvable, and this includes any incoming banks from the UK.

As a conclusion, the SRB recognises there is still a lot of work to do, but is committed to ensuring that, however financial markets may develop, we are able to meet our objectives and make banks resolvable.

CHAPTER 2

CASE STUDY 1: REGULATORY COMPLEXITY

'EVERYTHING SHOULD BE MADE AS SIMPLE AS POSSIBLE, BUT NOT SIMPLER.' A.EINSTEIN

The banking industry went through a wave of regulations over the past decade which has fundamentally changed the way banks operate. The reforms touched about every aspect of banking – prudential regulation on liquidity and capital requirements, market and trading venue reforms, organisational requirements, governance and conduct regulations – all with the aim to establish a more resilient, robust and safer financial system. The financial system is safer, but the volume and complexity of regulation have reached dizzying heights, and more rules are constantly added to an already multifaceted and baroque regulatory edifice. As policymakers and the industry gradually pivot from the rule-making phase to implementation and rule assessment, it's appropriate to consider the trade-offs associated with the quantum increases in regulatory complexity over the last years. Many new buttons were added to the cockpit to make the plane safer so to speak, but does the dashboard's extreme complexity now make the plane harder to fly, or more importantly harder to land in a crisis?

Accelerating regulatory complexity - The tower of Basel

First, let's consider the evidence of mounting regulatory complexity. Capital regulation is often quoted as the prime example of increasingly complicated rules. It may be somewhat superficial to focus on the length of applicable regulations, but it is nevertheless illustrative of the general concern. The first Basel accord in 1988 totalled 28 pages but this has swelled to 616 pages for the latest Basel III text. The implementing legislation is, of course, many times longer with 1000+ pages of domestic documentation which is again further inflated by many hundreds of pages of secondary and tertiary rules. It is said that you could compute a bank's capital requirements on the back of a postcard in the early '90s but by the time internal models were introduced in Basel II this became impossible with risk buckets proliferating into the hundreds of thousands resulting in hundreds of millions of capital calculations. It is positive that prudential regulation has moved from a relatively crude conception of risk (Basel I focused largely on credit risk) to a greatly enhanced framework, however, the price for the broader coverage has been added complexity (see Box 1). The density and versatile nature of modern capital regulation is increasingly questioned from both private and public sides.

'While I do not know precisely the socially optimal number of loss absorbency requirements for large banking firms, I am reasonably certain that 24 is too many.' R. Quarles, Federal Reserve Bank

'Regulatory capital ratios may have become too complex to verify, too error prone to be reliably robust and too leaden-footed to enable prompt corrective action.' A. Haldane, Bank of England

Box 1

Complexity in the capital stack

Capital components: Common Equity Tier 1 / Additional Tier 1 / Tier 2 / Capital Conservation Buffer / Countercyclical Capital Buffer / Systemic Risk Buffer / G-SIB buffer / Loss Absorbing Capacity / Pillar 2 & stress tests / Maximum Distributable Amount (MDA) etc.

Complexity in the 'simple' backstops to risk weighted capital: leverage ratios are not as simple as they appear and banking groups are subject to multiple different leverage ratios which can total more than 20 in some instances and apply at many different levels.

Outside of prudential requirements, complexity has increased across many other areas of financial regulation. The Markets in Financial Instruments Directive/Regulation (MiFIDII/MiFIR) is arguably one of the most sophisticated financial regulatory reforms yet; the implementation in many EU Member States runs to 5,000 plus pages and introduces far-reaching reforms across markets and trading venues. The increased complexity in traditional lending and markets-based fields of financial activity has also been compounded

in recent years by the introduction of new regulatory frameworks to cover emerging risks in new spheres, be they macro-prudential systemic risks, shadow banking concerns, or relating to newer phenomena like the increasing digitalisation of banking, or climate finance. The rising complexity and density of regulation have required both more supervisory staff on the public side (in the UK employees at regulatory bodies have tripled since 2000) and a huge increase in Compliance and Legal officers on the private side: one study on this topic notes that a major US bank has more staff in Compliance now (reportedly above 20 thousand) than the total number of Lehman employees at its collapse, and other reporting suggests another major US bank has more controls staff than there are police officers in New York.

Key drivers of complexity

At a basic level some see an elaborate regulatory framework as the necessary corollary to reflect an increasingly globalised, complex and non-linear financial system; regulation mirroring reality. Others reject this correlation, and in fact raise the precise risks of trying to regulate a complex system with complex regulation. Stepping back, we can identify several drivers of increasing complexity, which include i) events, ii) methodology/design, iii) dynamics and iv) application.

i. **In terms of events,** the financial crisis of 2008 ushered in a huge step-change in the volume and quality of financial regulation. Regulatory gaps were filled and many deficiencies remedied across prudential, markets/derivatives and governance. This re-regulation of global finance was certainly necessary, and all measures are individually well-intentioned, however, the unprecedented wave of reform has created a rulebook that is, in places, almost impenetrably complex.

ii. **Methodology / design:** in places, regulatory design mimics the Tinbergen Model, which stipulates that in order to control a desired number of targets, policymakers need to control an equal number of instruments. This is manifested in regulation as a distinct rule for every aspect which needs to be regulated. Combining the Tinbergen-like approach with the inherently reactive nature of regulation, means that for every aspect that needs to be regulated, one distinct rule should be implemented. Unfortunately, neither the causes nor the tools to control them are always distinct and uncorrelated, which means the more regulation, the more overlaps and unintended consequences.

   The way new regulation is added to the existing body of rules without the old provisions removed (for example the Basel I floor) can also create complications and in this sense regulatory complexity is a self-perpetuating process.

   We should also acknowledge that the laudable quest for risk sensitivity is also another driver of regulatory complexity; this process is itself fuelled by advances in technology, for example, the increasing parameterisation of capital computation is only possible due to sophisticated developments in quantitative modelling.

   Lastly, the design of major regulation rarely factors the multi-year implementation efforts necessary to embed it within organisations.

iii. **Dynamics:** regulation has to evolve constantly to keep up with accelerating innovation in the marketplace. This will become even more key as emerging technologies like Big Data, Cloud, Artificial Intelligence, and Distributed ledger transform business models across all aspects of banking and facilitate the emergence of new players, products and risks (e.g. cybercrime). Developing new regulatory guidance and frameworks to manage these developments (including anchoring them coherently in the current rulebooks) will be a challenging and complex task. Finally, there is clearly a cyclical dynamic related to the interactions of economics and politics that can create regulatory dissonance.

iv. **Application:** although a perfectly level playing field is an unrealistic prospect, major divergences in the implementation of globally-agreed regulation creates fragmentation and exacerbates compliance challenges in addition to reducing competition and creating systemic financial vulnerabilities.

   The application of financial regulation which is conceived at consolidated level, to all subsidiaries, which is a trend evident in the prudential sphere, can complicate the management and efficiency of banking groups.

The extraterritorial reach of nationally/regionally conceived regulation, which is increasingly becoming a characteristic in certain areas, for example anti-money laundering, data privacy and conduct rules, increase complexity which is multiplied where monitoring and policing of client activity is outsourced from regulators to banks themselves.

Finally, supervisory divergence also drives complexity for globally active regulated entities and contributes to unlevel playing field issues.

In summary, there are a range of powerful drivers of regulatory complexity, suggesting approaches to manage or simplify the current rulebooks will have to be varied and sustainable through the cycle.

Selective ongoing simplification

The generalised increase in regulatory complexity has not passed unnoticed as the quotes above from the regulators Quarles and Haldane evidence. The breadth and complexity of recent financial regulatory change have stimulated the new and welcome FSB G20 regulatory reform evaluation process, which aims to examine the effects of financial regulatory reform on financial intermediation. The FSB has started examining the impacts of infrastructure and leverage ratio reforms and will turn its attention to TBTF regulation in 2019.

At Basel, recognition of increasing regulatory complexity prompted the creation of a taskforce on Simplicity and Comparability in 2012, whose work was instrumental as regards the final Basel III standards, and there is a significant amount of work ongoing relating to enhancing disclosure and reporting.

The European Commission focused intently on the topic in its Call for Evidence in 2015 which assessed the cumulative impacts of financial regulation and need for more proportionality, which has informed recent legislative proposals including several so-called refit projects.

In the US there have been several efforts to streamline, tailor and simplify regulation – most notably perhaps, the current Chairman of the Commodity Futures Trading Commission (CFTC) famously named his 2017 simplification initiative 'Project KISS' – Keep It Simple Stupid.

Consequently, although the trend has been one of a very dramatic increase in regulatory complexity since the financial crisis, we should note that there is some selective and ongoing work to simplify rules, or at least to render them more comparable. Perhaps most strikingly, the latest Basel III standards that were finalised in December 2017, reacted to concerns about the complexity and lack of comparability across the banking industry of internally modelled risk-weighted assets. Some key features of the new package are designed to simplify capital computation:

- **Operational risk:** removal of the internal model, Advanced Management Approach (AMA) in favour of a revised standardised approach (Standardised Measurement Approach).
- **Credit risk:** removal of the IRB model for low default portfolios (banks, financials and large corporates) and moving them to Foundation IRB (only Probability of Default modelling).
- **Aggregate output floor** introduced across all risk classes and calibrated at 72.5% once fully phased in.

It is too soon to conclude, but these reforms do appear to have at least partially met the objective of simplification. Taking Operational Risk for example, the historical AMA model was complex and resource intensive to run, with the resulting capital number often not the most useful tool in terms of helping manage risk internally. However, quantification of risk is central to managing it, so now rather than spending time on a complex internal capital model, the risk professionals can work on the quantification of emerging operational issues like cyber and third-party risks in a way that facilitates more effective risk management.

That said, there are some noticeable trade-offs with this simplification. While the new formula within the standardised approach is simpler, it lacks the risk sensitivity of the AMA. For example, certain risk mitigation techniques like the use of insurance to cover potential future operational risk losses, which are fully recognised today as an Operational Risk mitigant, will no longer qualify as such under the new standardised approach. This could result in significant capital increases for banks despite the underlying risk profile remaining completely static. The inclusion of national discretion for some of the parameters also weakens the comparability objective to some extent.

The above-mentioned trade-offs bring to the fore the broader question around whether reverting to a radically simpler system is the answer to the

growing complexity of financial regulation. As noted, there are schools of thought, often taking their cue from other fields like environmental or health regulation, who advocate against complex controls for a complex system.

'Faced with complexity, the temptation is to seek complex control devices. In fact, complex systems typically call for simple controls. To do otherwise compounds system complexity with control complexity. Uncertainty would not then divide, it would multiply.' Haldane, 2011.

There are also academics who favour reverting to basic (and high) leverage and capital metrics. Although tempting at one level, these approaches contain some significant drawbacks, primary among which is the concern that 'blunt' risk insensitive approaches can result in a divergence between regulatory risk and economic risk. Internal risk management professionals may find themselves undertaking more of a 'compliance' function than a risk management one, with the latter outsourced to the regulators. This is worrisome from an accountability and ownership perspective, and clearly can create damaging incentives which may result in increased risk and less efficient capital allocation. Secondly, simple metrics are vulnerable to arbitrage, as happened following Basel I. Reverting to simple and standard rules can also disincentivise investment in increasingly sophisticated risk measurement and management systems. Finally, simplicity can often be superficial as mentioned in the context of the leverage ratio.

Concerns with complexity

If the drivers of regulatory complexity are multiple and likely enduring, and reverting to radical simplification also has its drawbacks, we should now turn to the main concerns with regulatory complexity.

Compliance: understanding, interpreting and complying with rules is increasingly challenging as complexity rises, particularly when in a cycle of continuous implementation. Compliance is rendered more challenging by the increasing interplay of different regulations (overlaps and conflicts in particular). Whether it is balancing leverage and LCR constraints, managing data privacy rules against AML reporting requirements, or designing a Single Point of Entry strategy in an increasingly ring-fenced world, there are rising instances of well-intentioned solo regulations that create tension with other elements of the rulebook.

Complexity and compliance issues also arise when hot policy topics are addressed by multiple policymaking agencies through a diverse set of legislative instruments; consider the important issue of Environment, Social and Governance factors on which the EU is playing a leading role. Currently we see new ESG requirements proposed in the Banking Package (CRRII, CRD4), in the Investment Firm Review, in the standalone Disclosures file under the Sustainable Finance Action Plan, via recent consultation papers from the European Securities and Markets Authority (ESMA) proposing changes to MiFIDII, the Alternative Investment Fund Managers Directive (AIFMD) and the Undertakings for the Collective Investments in Transferable Securities (UCITS) Directive, and we shortly expect the topic to be revisited in the context of MiFID suitability rules.

Management: steering a bank amid a forest of complex metrics is demanding on management and can be risky in times of crisis. It is increasingly challenging for any one person or group of people to understand the holistic risk framework. In a going concern it is also problematic to determine the effective binding constraint where an activity is subject to multiple control mechanisms (e.g. risk-based capital, input & output floors, leverage ratios, and stress tests / Pillar 2). There are also now instances of where new rule sets are starting to override old ones – take for example resolution planning through which the capital and liquidity requirements for material legal entities and associated ring-fencing start to prevail over traditional prudential capital and liquidity regulations. Legal entity complexity (where this is encouraged by law or supervision) has also created issues both with the ring-fencing of capital and liquidity which heighten the risk of failure, but also as regards governance and decision-making between subsidiaries and group.

Costs: legal and compliance costs have skyrocketed over the last decade. Credit Suisse Bank analysts estimate that L&C costs for European banks have been growing at around 20% – 30% for several years (slight deceleration in last 1.5 years) and now account for 7% – 9% of total operating expenditure. Some of the significant increase in costs can be justified, but conversely where extremely high costs depress return on equity there are also negative longer-term consequences. Perhaps more importantly, the increase in cost creates barriers to entry into the market, which results in some activity displacement outside the regulatory perimeter and to distortions in competition. We estimate the reduction in Foreign Banking Organisation (FBO) broker dealer activity in the US post-crisis

(down ~60% according to some estimates)[24] results in part from high regulatory costs.

A general concern related to the nature of regulation is increasing opacity. If complexity and information asymmetry impede market transparency, then price formation as regards banks' equity and debt capital instruments are challenged, and ultimately market discipline eroded. An additional general effect of excessive regulatory prescriptiveness may be rising homogeneity of banking business models (among traditional incumbents), whereby such 'herding' can give rise to monocultures where risk-reducing diversification is displaced and contagion risks increase.

Options to consider

Addressing regulatory complexity is no easy task. The Basel Committee has concluded that retaining a mix of risk-based ratios and non-risk-based indicators for bank solvency is the right approach. This seems logical if we wish to retain risk sensitivity while increasing comparability. However, there is likely further progress that can be made to delay and simplify some of the key prudential metrics within such a framework. Reducing the number of solvency metrics in the US from 24 down to a more manageable number seems obvious. In the EU, the new Banking Package sets out requirements for loss-absorbing capacity for G-SIBs and Top Tier banks. This is a fundamentally important requirement and welcome regulatory progress. Due to a fraught political process, however, the final rules for both the quantity and quality of MREL are almost impenetrably complex when you factor both Pillar 1 and Pillar 2 requirements which themselves are calibrated subject to a mix of ratios and which include a convoluted system of caps, carve-outs and discretion. Further down the line it may make sense to review this system if evidence suggests there is a complexity premium for EU banks relative to others.

The complexity arising from regulatory divergence across jurisdictions is being addressed by Global Standard Setters to some extent, and we included several policy recommendations on this topic in our Discussion Paper from last year. In short, increasing ex ante regulatory coordination on future regulation, and a feedback loop to debate proposed regional divergences at the global level following adoption of standards would both foster increased convergence and limit the complications of divergent rule sets.

As noted above, the regulatory reform evaluation process, spearheaded by the FSB but encompassing Basel, the Committee on Payments and Market Infrastructure (CPMI) – International Organisation of Securities Commissions (IOSCO) too, is a very welcome step and should help identify areas of regulatory duplication, overlap and incoherence. The work undertaken to date has targeted some vital areas, and the upcoming review of Too-Big-To-Fail will be important. Consistent with the pivot from rule-making to the implementation from a strategic perspective, it is important that both public and private sector stakeholders are able to resource these areas sufficiently so that the volume and coverage of these initiatives can be increased over the coming years.

Supervisory convergence, via less national discretion and increased collaboration is an important area as regards regulatory simplification, as is the increased use of supervisory judgement to offset the need for prescriptive regulatory requirements at an excessively granular level. These are areas where the EU and the Single Supervisory Mechanism (SSM) in particular are focused and delivering important results. We would also recommend, where possible, that major new regulatory reform initiatives take account of the implementation and project delivery complexity that firms are faced with when final rules are published. There may be instances where leveraging project management expertise at an early stage of the policy development phase can result in changes to sequencing or phase-ins for final rules that would facilitate industry compliance.

It may also be worthwhile to consider a practical way to segment regulatory reform into areas where varying levels of complexity are warranted. We may, for example, distinguish between:

1. Requirements to ensure a stable system, where individual entities can fail, but the system needs to stay intact;

2. Conduct rules which need to be adhered to at all times, and;

3. Agent rules, where banks act or enforce on behalf of authorities.

For the first category, simplicity within a risk-sensitive framework would be desired (encompassing prudential and TBTF regimes). For the second, more prescriptive measures may

be warranted, and for the third a pragmatic and collaborative approach is preferable.

As concerns grow about the incremental benefits to financial stability or investor protection from an increasingly complex regulatory framework, an enhanced focus from both banks and supervisors on internal risk culture may deliver strongly in terms of value for effort. Individual accountability can be a strong element of the overall risk framework, and the introduction of the Senior Managers' Regime in the United Kingdom (UK), sets an interesting precedent in this area.

Finally, there are some very promising technological developments that may support efforts to manage both regulation and compliance complexity (see Box 2). For example, RegTech allows for new ways to regulate, reduce duplication and remove inconsistencies in interpretations, ultimately making numerous complex regulatory processes more efficient and effective. Banks and regulators should continue to invest and collaborate intensively on such projects which may offer the opportunity to effect radical change in the relatively short-term (see Box 3).

Box 2
Tech to help manage regulatory reporting complexity

On average, one regulator alone receives thousands of pages of regulatory reports from a financial institution per year. Financial services firms have hundreds of employees working on reporting to regulators with an average spend of over EUR 150m annually. Regulatory reporting is not just voluminous and costly, other frequently raised challenges relate to duplication, interpretative issues and vagueness, data quality and time lags.

Using technology to turn regulations into machine-readable code is one way the industry is looking to reduce cost, increase efficiency, and streamline reporting. Technology could improve reporting accuracy and render it almost instantaneous, reducing a time lag that can be weeks in some cases to a 30-second reporting timeframe. Reporting requirements in machine-readable format would substantially reduce the effort and cost of implementing new reporting requirements. Six banks along with two regulators have piloted the Digital Regulatory Reporting (DRR) aiming '...to make Regulatory Reporting seamless for both firms and regulators, by implementing a shared solution to support the automatization/digitisation of current manual processes. It will improve the communication of regulatory intent, remove inconsistencies in interpretations, and reduce duplication of data across the industry, making the entire process more efficient and effective.' The pilot this year demonstrated how future machine-readable rules could be transformed into reporting code, written by the regulator, and distributed to Firms' architecture over Blockchain. The Machine-Executable Regulatory Reporting (MERR) code can then consume a Firm's data through an Application Program Interface (API) to perform compliance calculations, without a Firm having to build its own compliance code.

Furthermore, financial institutions increasingly make use of machine-learning and data science-based methods such as clustering, matching, scoring or network algorithms to target effective, efficient and compliant implementation of regulatory commitments and requirements and to reduce the often significant number of false positives in monitoring processes (e.g. surveys in the AML space report false positive rates of more than 90 percent). Forward-thinking institutions employ such methods in the space of Client Monitoring and Employee Surveillance. In an effort to drive innovation in this space, many major banks frequently demonstrate to, and get feedback from, various regulatory agencies on newly developed solutions, and support and facilitate discussions about data-driven technological solutions whenever appropriate.

Box 3
Areas to consider for selective regulatory simplification

1. **Recovery and Resolution Plans:** Recovery and Resolution Plans (RRPs) for large G-SIBs run to thousands of pages. We are long advocates of solving TBTF, which at its core consists of ensuring there are workable mechanisms to convert sufficient loss absorbing capacity into equity without creating systemic cross-defaults. You need the principles, resources, and legal powers to do this work, and these are largely already in place (more clarity is required on funding in resolution, however). The question is around the usefulness of long-form RRPs in a crisis, when both bank management teams and resolution authorities will be in urgent need of a short and simple manual to help effect a capital transformation in a compressed time period. Such 'presumptive paths' may be considered as a complement or partial substitute for complex RRPs.

2. **Ring-Fencing / subsidiarisation:** The trend towards geographic ring-fencing and compartmentalisation of banking groups, allied to the application of prudential regulation (e.g. liquidity ratios) at sub-consolidated levels, gives rise to additional complexity and several significant concerns related to decreases in group resilience, and reduced efficiency in the allocation of capital. This topic of fragmentation would be best considered at global levels, and we welcome the focus on this from the incoming Japanese Presidency of the G20.

3. **Capital buffers:** post-crisis regulatory reform has seen a marked increase in the number of buffers added to capital and leverage requirements at both Pillar 1 and Pillar 2. The complexity of buffers, the role they play (are they de facto new minimum requirements or can they be drawn down?), and the heterogeneity between jurisdictions on this topic (for example as relates to macro-prudential buffers) would merit re-examination for ways to simplify the framework. The new focus of the Basel Committee on this topic and the usability of buffers in particular is most welcome.

Final remarks

Regulation is vital to safeguard financial stability and protect investors, and recent regulatory developments have transformed the financial system for the better. The challenge is to ensure regulation is effective as the volume and complexity continue to rise. Complexity makes the system harder to understand, and potentially more dangerous in the next crisis as banks become harder to supervise and manage. It is too late to turn back the clock and reinvent a radically simpler system, and in many ways such a paradigm would likely remain suboptimal for the reasons outlined in this case study. As regulation continues to evolve to address risks in new areas, it will remain important to ensure ongoing review to assess the trade-offs necessary to strike the right balance between risk sensitivity, comparability and simplicity. We support ongoing efforts to selectively de-complexify regulation, with the ambition not to reduce capital requirements per se, but with the aim to ensure regulatory outcomes are achieved in the most effective manner. Such a path forward would include:

1. Developing a framework to categorise risks and the optimal granularity of rules necessary to mitigate them;

2. Undertaking targeted simplifications where unintended consequences are evident (see Box 3);

3. Stepping up regulatory review and assessment of financial regulations (including analysis of interplay and duplication), and;

4. Investing in innovation (RegTech) on both public and private sides to identify how technology may both accelerate the simplification process and also facilitate better management of complexity.

BOX

*Statement by **Sadie Creese,** Professor of Cybersecurity, University of Oxford*

Cybersecurity – intervening for future resilience

The financial sector has always taken a lead on addressing the cyber risk, and so it is particularly important that this community consider whether there is a need to do more collectively in ensuring continued resilience in the face of evolving cyber-threats.

There is little question that the benefits of digitisation are significant, and that, in general, assuming we can practice effective risk management, history has shown that the positives dwarf the costs of managing the cyber-risk. Of course, this may be evidence of how resilient the sector has been (or it may be that the cyber-value-at-risk was never actually that high). The crucial question we must ask ourselves is whether, using current practice, we can maintain this position given the rapidly changing environment in which we operate.

The continued growth in dependency on digital throughout the financial sector, and the customers it serves, makes it a target for cyber-attack; it creates an ever-evolving attack surface across which a myriad of harms may manifest – not least theft, sabotage and reputational damage. The maturity of the ecosystem within which cyber-assets gained from attacks can be monetised means that we face a motivated, sophisticated and skilled community of adversaries, who are comfortable working outside the law, and who benefit from the global nature of cyber-connectivity to avoid easily being prosecuted for crimes. Add to this a component of state-sponsored or state-sympathetic cyber-attacks which also stimulate the development of sophisticated cyber-weaponry and trade-craft.

The combination of constantly evolving attack surface, with motivated, sophisticated and well-resourced threat actors, and dependency upon cyber to conduct business, means that the Cyber Value-at-Risk is potentially very high. Further, the commonality in features and interconnectedness of our digital infrastructures (not, unfortunately, matched by a commonality of national regulation) means that we may well be exposed to growing systemic risks across the financial sector and beyond. It is highly likely that any response to such systemic risk must match the scale in order to be effective. The alternative would be to try and protect our organisations separately, acting independently, requiring a level of heterogeneity across our systems that would directly impede business. In other words, to address system-level risk we will need to act as a system – working together.

Current best-practice always evolves in response to our body of experience, and ensuring that we can collectively share knowledge will protect this function. Of course, specific risk controls that require us to have good intelligence on threats, their capabilities, and the nature of attacks we may face in the near future, will all have very specific requirements for sharing of information. Sharing to build a common situational awareness is a capacity that we must always seek to improve. This is not a new observation, but will require continued and persistent efforts towards improvement in collaboration across the sector, both in sharing threat intelligence, and in aligning the various regulatory regimes that determine best practice for response. Indeed, if we are to try and anticipate threats we have not faced before, then arguably we should seek to develop trusted relationships for sharing threat intelligence outside the financial sector – in order to benefit from a more diverse range of experiences of cyber-attack. Of course, a systems scale response would need to go beyond simply the sharing of threat intelligence. It will likely need to involve threat detection systems, harm propagation methods, situational awareness tools and ultimately proactive cyber-defence.

However, there is a case that relying on well-resourced evolution of best-practice and stronger collaborations is not going to be sufficient to deliver ongoing resilience; the scale of change in our cyber-operations, technology and threat landscape, calls into question whether more novel and creative solutions may be required. For example, the Internet of Things (IoT) is rapidly developing and, whilst estimates vary on the exact volume of computing devices likely to pervade our future environment, there is broad agreement that we will reach a measure of billions. But in a world instrumented to this level it is difficult to see how current risk controls can scale. Can we deploy access control across a population of devices so large? Will we even know where our perimeter is? And if we do, how quickly will that view become out-of-date as the dynamics of the devices lead to a constant shifting in network configuration. Regardless of which markets succeed, and which fashions take hold, we simply will not be able to depend upon perimeter-based security controls; it is not realistic to assume we can keep the malign out.

Consider then insider threats. They are not new, and the belief is that the volume of cyber-attacks being conducted using insiders for some element of an attack are actually much larger than is reported. Insiders can develop deep insight into our systems, which can lead them to cause very significant harm. Insiders also have the benefit of serendipity that persistent access to systems can provide; they may enter looking to cause one type of harm and discover something more that can be achieved. So a question we must ask ourselves is whether our cyber-security systems are well positioned to detect insiders. The answer is that even for today's systems it is very difficult– how might that be worsened in a future environment where we have much more complex systems of devices? If the IoT makes boundaries blurred and hard to maintain does that mean that all threats are effectively insiders? Does it matter that the bulk of our current defence mechanisms are predicated upon boundaries and access controls?

Of course, IoT and Insiders is just an example of how a technology trend is going to shape our environments in such a way that calls into question our current tools for managing risk. Others we might consider include the use of machine learning and the potential for toxic learning that could introduce new risks (such as biased decision systems) or cause old risks to grow (imagine an attacker who can utilize machine learning to predict our cyber-defence mechanisms in such a way that they can avoid detection). Or perhaps the growth in use of distributed ledger technologies and digital currencies might lead us to take positions in the market that create an exposure so great that a single attack on the integrity of these systems (and there is a growing body of knowledge on potential vulnerabilities) might actually prove toxic to other lines of business. How will we detect malign learning, or influence, or attacks on digital ledgers?

When we consider the future and what it means to be resilience as a sector, as organisations, or as cyberspace, then we ought to be asking ourselves: What kinds of residual risk will we be carrying after we've deployed the best protections at our disposal? Could it be systemic, realised within a unit of time that could cause catastrophic failures in our systems? Do we have the capabilities to detect the risk as it begins to be realised? Can we estimate the consequence – the harms that may result?

We are, as a community, working to develop an understanding of what our real Cyber-Value-at-Risk might be. But the current position is that we lack the data to really evidence and quantify the effectiveness of security controls in reducing risk; we rely on experience and trade-craft. This means that it is exceptionally difficult to quantify or size the risk – and more must be done to align the different practices. Likely we will need to increase the scope of what is measured in order that we might fully qualify our risk and deepen our understanding of the harms that occur as a result of a lack of cyber-security.

The costs that can result from an incident can continue to grow long after an incident is determined to have taken place, and, in many cases, it is the investigation into what else may have occurred and how to prevent similar attacks happening in the future, that is the larger cost component. Where we are using cutting edge

technologies you can expect our response and recovery costs to be correspondingly high; similar technology and methodology complexity will be required to perform the security analytics necessary to direct recovery and inform learning. We need the ability to determine what is happening and what might happen, how risk might be manifesting, how it might propagate and cause harm, and how our responses are acting to minimize loss.

The nature of risk management practice, including cyber, necessarily requires that we have an ability to identify the risks that we wish to treat. Will we be able to anticipate the threats and have access to the controls required to effectively mitigate the future risks? Or are there new interventions and capabilities we need to be making and developing now in order that we can remain resilient? There are many questions that we must address if we are to take reasoned positions in support of our future cyber-security, and many questions that we may need to answer in order to convince ourselves that our future investments are secure in the face of cyber-threat.

CASE STUDY 2: CYBERSECURITY

As the financial sector progresses towards unprecedented levels of service digitisation and technology-driven back-office automation, the management of technology and cyber-risks continues to receive substantial attention from both the industry and regulators.

On the business side, the sector's dependence on technology is unprecedented. Clients expect seamless and secure omni-channel, cross-border products and services. Financial institutions are using innovative technologies to manage complex data and reduce operating costs. Digital capability has thus become one of the key elements of competitiveness within financial services, bringing along a spectrum of challenges for individual institutions and potential risks to the financial system as a whole. Technology change management has become a key component of managing these risks.

Proactive technology risk management is now a priority across banks' operations. Cybersecurity – including the prevention of fraud, data breaches and business disruption – is now recognised by senior management as critical underpinnings of stable and accessible business. Boards are paying attention to anticipating, preventing and managing cyber-related exposures and protecting the assets of their respective institutions. The risk is now recognised as reaching beyond institutional perimeters and encompassing third party (and even fourth party) relationships.

A **cyber risk** has been defined as 'the combination of the probability of an event occurring within the realm of an organisation's information assets, computer and communication resources and the consequences of that event for an organisation' (The CPMI-IOSCO Guidance - 2016).

However there is an increasing appreciation that this may be too narrow a definition and that the risk now extends beyond organisational boundaries.

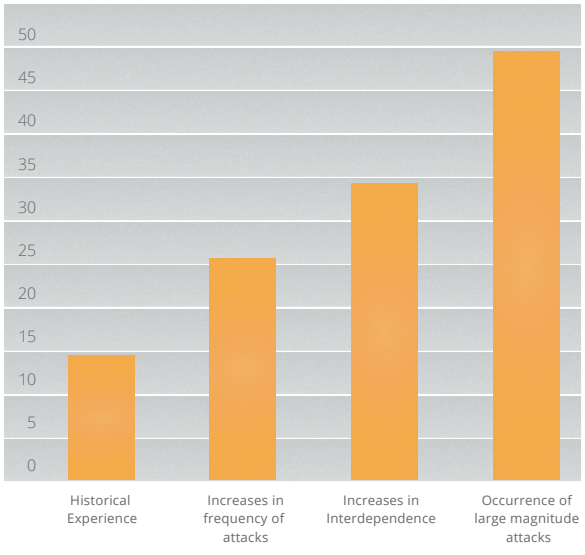
Regulators view cyber resilience as a pillar supporting the systemic stability of the financial sector, recognising that a successful attack on a leading institution could have a substantial impact on both consumers and financial markets. In a recent report, the BIS concludes that several countries have recognised the need to set out clear rules to protect their jurisdictions – notably China, Hong Kong, Singapore, the United Kingdom, and the USA – and have introduced related guidance in recent years.[25]

Sizing the risk

There are multiple estimates, from both private and public sector institutions, addressing the costs and potential losses resulting from cyber threat to the financial sector. One recent assessment by Accenture suggests that the cost of cybercrime for financial services companies globally is rising steeply, increasing by over 40% between 2014 and 2017 (from USD 12.97 million to USD 18.28 million per firm). This is nearly double any other sector. Business disruption and information loss comprise 87% of the cost, with revenue loss estimated at 13%.[26] The International Monetary Fund (IMF) estimated, conservatively, that the total average annual cost to the industry equals approximately 9% of its net income, or USD 100 billion (Figure 5). The IMF suggested that potential losses of this magnitude represent a possible threat to global financial stability.[27]

Figure 5: Potential impact on bank profits

Financial institutions worldwide face potential losses from cyber-attacks ranging from 9% of net income based on experience so far up to half of profits in the worst-case scenario.
(percent of net income)



Source: IMF

There is broad agreement among key stakeholders that a successful attack on an internationally active bank or market infrastructure provider could cause a shock across one or multiple markets. The financial sector is:

1. Particularly exposed to cyber-risks, as it relies heavily on IT-infrastructure and in-time access to information;

2. Strongly interconnected as an industry, but also with other sectors (through payment systems); and

3. Critical for the functioning of the overall economy as a key enabler of economic growth.[28]

The International Organisation of Securities Commissions echoed this assessment in 2016: *'cyber-risk constitutes a growing and significant threat to the integrity, efficiency and soundness of financial markets worldwide'.*[29] IBM reported that, in 2017, financial services were for the second consecutive year globally experiencing more cyber-attacks than any other industry, and were the target of cyber-attacks in 27% of cases.[30] IBM added that the focus of cybercriminals has turned from data theft towards launching ransomware and destructive attacks with the aim of blocking or destroying the owner's information.

The insurance industry is grappling with similar challenges to measure and size the potential impact of technology and cybersecurity risks in order to play a role in providing accessible risk policies.

Current regulatory practices

Cybersecurity is high on the agenda of financial regulators. Important national and supranational regulations and guidelines have been issued in recent years (see Table 1 for an overview of key European regulatory initiatives).

In October 2017, the World Bank finalised a review of current cyber-risk regulatory practices and identified no fewer than 56 substantial national and supranational efforts.[31] The FSB described similarities and repetitions across jurisdictions, with *'many of the same topics addressed, including governance, risk analysis and assessment, information security, expertise and training, incident response and recovery, communications and information sharing, and oversight of interconnections.'* [32] Different oversight institutions have taken different approaches, in part because the rapidly evolving scale and complexity of cyber-related risks is challenging to capture in regulatory terms. Some regulators prefer to subsume the topic within existing technology and operational risk frameworks, which may prevent legal language from becoming obsolete over time, or having to be continuously reviewed and adapted. Others have adopted a more dedicated approach and regulatory agenda. There is limited consensus across jurisdictions on the appropriate level of detail and specificity of the rules. Banks are required to provide critical information, their resilience is regularly tested in a controlled environment, and there is an increasing expectation of clear and transparent responsibilities as well as a dedicated cybersecurity policy framework, including provisions for contractors and other third parties.

Financial institutions are also clearly in scope for increasing personal data protection regulations such as the European General Data Protection Regulation (GDPR).

Two key principles might be considered by national regulators:

- **Cybersecurity risks and their impact need to be considered specifically when introducing new financial regulations.** For example, the EU-Payment Services Directive II has forced banks to allow their customers to share their financial data (such as spending habits and regular payments) with authorised third-party providers. While introducing valuable benefits to financial sector customers, in this case through increased accessibility and transparency, this also presents new data protection risks which need to be thoroughly assessed.

- **Consistency in national regulatory measures and international collaboration.** Regulatory oversight of cybersecurity needs to be consistent and harmonised in order to avoid either clashing demands or an undue regulatory burden that paradoxically undermines technology risk management. Collaboration needs to take place in a clearly defined environment in order to prevent miscommunication or increase information gaps between regions and jurisdictions.

Table 1: Selected European and supranational regulatory and law enforcement efforts in addressing cyber-risk in financial services, listed by date issued/launched

INSTITUTION / GROUP	ACTIVITY
European Union Agency for Network and Information Security	Since 2004, the European Union Agency for Network and Information Security (ENISA) has been Europe's dedicated competence centre in the area of cybersecurity. Among its activities are the development of National Cyber Security Strategies, cooperation and capacity building, privacy-enhancing technologies and privacy on emerging technologies, eIDs and trust services, and identifying the cyber-threat landscape. In October 2018, ENISA published its first full-year annual report on security incidents with electronic trust services. The recent adoption of the EU Cybersecurity Act empowers ENISA and transforms it into an EU Cybersecurity Agency that will notably govern an EU-wide voluntary cybersecurity certification framework for Information and Communications Technology (ICT) processes, products and services.
Europol	As early as 2013, Europol launched the European Cybercrime Centre (EC3) in order to facilitate law enforcement collaboration and joint efforts with regard to cybercrime. Among other activities, EC3 publishes an annual flagship report (Internet Organised Crime Threat Assessment), which includes data on current and emerging cyber threats. In 2014, a dedicated Joint Cybercrime Action Taskforce (J-CAT) was established, aimed at supporting and coordinating the fight against online crime, including high-tech crimes, facilitation of online crime and online fraud.
European Commission	In 2013, the European Commission adopted a number of legislative proposals to tackle the 'fragmentation of the EU cybersecurity market'[33] and allocated substantial funds (approx. EUR 600 million) for future research and innovation in cybersecurity projects by 2020. Among the key pieces of legislation adopted by the Commission is the Directive on Security of Network and Information Systems (NIS Directive) of July 2016. At the same time, the Commission launched a public-private partnership on cybersecurity, committing EUR 450 million under its research and innovation programme Horizon 2020. As part of its Action Plan on Fintech, the Commission has also invited the ESAs to report on the existing supervisory practices around ICT security as well as on the costs and benefits of developing a cyber resilience testing framework that can be applied to all significant financial players. The GDPR represents a substantial overhaul of privacy law and redefines data protection and privacy rules across Europe, including stringent global requirements around personal data management and protection, strengthening the privacy rights of EU citizens. From a cybersecurity perspective, GDPR requires the adoption of sufficient technical and organisational measures in order to provide for adequate data security. It also requires businesses to report cybersecurity breaches to authorities within 72 hours, or face severe fines (up to EUR 20 million or 4% of global annual revenue, whichever is higher).
Group of 7	On a global level, the Group of 7 (USA, Japan, Germany, the UK, France, Italy and Canada and the European Union as a 'non-enumerated' member) adopted several elaborate strategic documents focusing on cyber during its 2016 summit, and consequently established the Ise-Shima working group on cyber. It adopted a common set of 'Principles and Actions on Cyber', committing itself to *'take decisive and robust measures in close cooperation against malicious use of cyberspace both by states and non-state actors, including terrorists'.* [34]

INSTITUTION / GROUP	ACTIVITY
Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions	In April 2016, these two organisations issued 'Guidance on cyber resilience for financial market infrastructures' [35], which introduced supporting information around establishment and operations of a cyber resilience framework. The document was the *'first internationally agreed guidance on cybersecurity for the financial industry'*, with the aim to *'support consistent and effective oversight and supervision of Financial Market Infrastructures (FMIs) in the area of cyber risk'.* [36]
Financial Stability Board	In 2017, the FSB identified cybersecurity as one of the three key priority areas for future international collaboration and included the need to monitor cyber-risk and address regulatory issues, notably with a financial stability perspective. In July 2018, the FSB published a draft 'Cyber Lexicon'[37] for public consultation, which comprises 50 core terms related to cybersecurity and resilience in the financial sector, aimed at establishing a cross-sector common understanding of relevant terminology.
European Banking Authority	In 2017, the European Banking Authority (EBA) published its 'Guidelines on the management of information and communication technologies risks for institutions' [38], which aim to promote common methodologies for the assessment of cyber-risk. Importantly, these guidelines do not introduce a new additional reporting obligation for institutions, however, they empower national authorities to request relevant information.
Joint Committee of the European Supervisory Authorities	In April 2018, the Joint Committee published a dedicated report, stating *'cyber risks threaten data integrity, data confidentiality, data protection and business continuity'*, and warned that *'insufficient protection against cyber incidents [...] could lead to major damages for financial institutions concerned, and potentially to the wider financial system'* [39]. Going forward, ESMA will proceed with supervisory convergence activities, as well as direct supervision, while also launching a supervisory project on cloud computing.
European Central Bank	In May 2018, the European Central Bank (ECB) set up the first European framework to test the cyber-resilience of financial market infrastructures (TIBER-EU). Further, the ECB has put in place a cyber-incident reporting framework, so that all significant institutions from the 19 euro area countries report significant cyber incidents. Also, the ECB has initiated the Euro Cyber Resilience Board for pan-European Financial Infrastructures, which raises awareness of cyber-resilience, facilitates joint initiatives to develop effective solutions for the market and encourages sharing of relevant best practices and fosters collaboration.[40]
National Cybersecurity Strategy Guide, co-issued by the International Telecommunication Union, the World Bank, Commonwealth Secretariat, the Commonwealth Telecommunications Organisation, and NATO Cooperative Cyber Defence Centre of Excellence	A major milestone and key supranational effort was successfully finalised in 2018, when the 'National Cybersecurity Strategy Guide' [41] was developed and published by twelve stakeholders from international organisations, private sector, academia and civil society to provide an internationally harmonised set of principles and best practices in developing, establishing and implementing national cybersecurity strategies.

Private sector efforts

Financial institutions recognise that they represent attractive targets for cyber adversaries and the financial sector is broadly recognised as being ahead of many other business sectors in mitigating the threat. Cybersecurity is a standing agenda item for senior management and boards. The financial industry has invested in training and awareness activities, cybersecurity technical controls and testing, and by recruiting senior cybersecurity experts. They have built capabilities to face complex cyber-risk scenarios. There is improving awareness of the risks posed by third party providers as potential entry points for cyber adversaries.

The finance industry has called for regulation that is more effective. In 2015 the Institute for International Finance (IIF) proposed to consider the Financial Action Task Force (FATF) as a reference for supranational cybersecurity cooperation.[42] The IIF established a dedicated Cybersecurity Working Group to assess cyber-risks. Their 2018 report highlighted regulatory fragmentation and asked the Financial Stability Board to aim for more consistency and coordination among regulators.[43] In Europe, the European Banking Federation (EBF) has been active in formulating the industry's priorities for effective regulation and collaboration, stressing the need for public-private partnerships and the exchange of information about cyber incidents among impacted institutions. The EBF highlighted a significant volume of cyber-attacks originating from countries not fully committed to judicial cooperation.

More recently, the need has been recognised to extend beyond a preventative perimeter-based defensive strategy to a more pro-active threat-led approach, with a particular emphasis upon operational resilience and the importance of developing response strategies that are appropriate for the specific threats posed by cyber events. Some firms are also working more closely together (and with public authorities) to improve their strategic insights into the activities of threat actors, and using this to identify potential pre-emptive prevention and disruption opportunities.

Cybersecurity culture - an organisational priority

A consensus is growing against treating cybersecurity and technology risk as simply a problem for the IT Department. Enterprises focus more and more on developing a people-centric corporate security culture fostering awareness and education for staff and third parties from Board level down. This is about what is done 'behind closed doors' - beyond that which is mandated or stipulated in corporate guidelines. When it comes to cyber risks, corporate culture needs to take into account what is said, done and valued at all levels.

Underinvestment in the human dimension of cybersecurity represents a significant risk factor: any technology risk remediation programme adopted must balance technical solutions with soft, human-centred skills. 'Social engineering', whereby human weaknesses and vulnerabilities are leveraged by adversaries, plays a significant part in the vast majority of successful cyber-attacks. This is in addition to the threat from the malicious insider, which requires concerted effort to manage.

Traditional regulatory approaches, involving in part little more than box-ticking mandatory online compliance programmes and formal policies, are unlikely to suffice in coaxing staff to consider, measure and understand how to address these risks. Awareness needs to be focused on 'people-centric security' and move beyond simple reliance on the existence of security policies and technical controls.

It is challenging both to influence behaviour change and to identify a way to measure cultural change; but it can be done. Moreover, firms will need continuously to evolve innovative messaging using dynamic channels. This might include Cyber Ambassadors, Digital Champions, community initiatives, interactive events, traditional (i.e. printed) as well as online communications. Done well this represents an effective and efficient use of defensive spending. People can be transformed from the weakest to the strongest link in the security chain. Underinvestment in the human factor of cybersecurity will be a significant risk factor and any programme adopted must leverage both the technical and soft, human-centred skills.

Summary

To counter this evolving threat, policymakers and regulators will need to work in close alignment both with each other and with the private sector. To be most effective, efforts should encompass people, governance, and technology. The scope will need to extend outside institutional boundaries to third parties, including suppliers, partners, and clients.

The effectiveness of cybersecurity rules and regulations will largely depend upon functional and collaborative partnerships between jurisdictions. Just as with complex financial regulatory requirements, cybersecurity regulation can become a burden on businesses unless applied with a high level of pragmatic consistency. To this end, the following will require particular attention:

1. **Common infrastructure and intelligence sharing:** banks should identify ways collectively to assess and protect shared infrastructure, including that provided by shared suppliers, many of which provide services across the industry.

2. **Consumer protection:** banks have invested substantial effort into protecting their IT infrastructure. However, new technologies, bank employees, clients and third-party workers represent an attractive point of entry for cyber-attackers.

3. **Corporate Governance:** Board level involvement in prudent technology-related decision-making and oversight is essential.

4. **Regulation:** financial regulatory efforts aimed at higher user convenience and transparency (e.g. the EU Directive on Payment Services) should also consider the consequences for cyber-risk and personal data protection.

5. **Cross-border standards:** should an institution with cross-border activities be subject to an attack, regulators need to be prepared to act consistently and to collaborate closely prior to, during and in the immediate aftermath of an incident. In practice, individual jurisdictions will need to collect information around cyber-attacks consistently and coherently, so that the data can be not only used to protect customers, but also shared to protect the stability of the financial system. Consideration should be given to how governments and the private sector might work together to reduce the volume of cyber-attacks originating from countries not fully committed to judicial cooperation.

CASE STUDY 3: CLIMATE CHANGE RISKS

Concerns about climate change, its (human) causes, and its severe consequences on flora and fauna have existed for decades in academia and the general public. So, strictly speaking, climate change risk is not an emerging risk. However, while individual financial institutions may have long begun taking climate change into account in their firm's risk management, the debate about the more systemic role of the financial system in either mitigating or exacerbating the trend and the potential implications for financial stability resulting from the financial impacts of transition ('stranded assets') or physical risks is a more recent one.

In 2015, before the Climate Conference in Paris, Mark Carney, Chairman of the Financial Stability Board (FSB), for the first time identified climate change as a priority in the FSB reform programme going forward, arguing that the potential risks to the financial sector from climate change are complex, growing, and should be better understood.

The Paris Agreement itself then outlined the need for greater mobilisation of financial assets to combat climate change, in particular private means. As an example, getting the right infrastructure in place would be one of the core elements to achieving a low-carbon economy. 70 percent of greenhouse gas emissions come from infrastructure such as electricity generation, transportation, industry, and buildings (Meltzer, 2016). In the report 'Better Growth, Better Climate' (2014) the Global Commission on the Economy and Climate estimates that USD 93 trillion would be needed from 2015 to 2030 to transform the world's infrastructure into a sustainable and ecological one. While this looks like an enormous amount, the estimates suggest that that the largest part, approximately USD 89 trillion, would have to be invested in infrastructure globally irrespective of any specific carbon emission reduction goal.

With these developments, the realisation that climate change not only poses a threat to financial stability, but also that the financial system needs to be transformed to better redirect financial asset flows to combat climate change, started to gain increasing traction within the industry and among regulators.

Response to climate change risk by financial institutions

In his speech on 'The tragedy of the Horizon' in September 2015, Mark Carney warned of three main ways in which climate change may affect financial stability:[44]

- **The physical risks** that arise from the increased frequency and severity of climate- and weather-related events that damage property and disrupt trade;
- **The liability risks**[45] stemming from parties who have suffered loss from the effects of climate change seeking compensation from those they hold responsible; and
- **The transition risks** that can arise through a sudden and disorderly adjustment to a low carbon economy, primarily driven by regulatory and technological changes.

On an individual level, banks have started to incorporate these risks into their risk management processes and assessment of products and services. A 2017 report by British investors Non-Governmental Organisation (NGO) ShareAction, 'Banking on a Low-Carbon Future', analysed the strategies and activities of Europe's 15 largest banks to manage climate change risk and shape the transition to a low carbon economy. The report found that all banks surveyed have considered climate-related risks and opportunities and adopted respective policies. However, it also pointed out that the most complicated areas of risk assessments and management, together with the development of low-carbon products and services at scale seemed most challenging for most banks. Separately, the UK Prudential Regulation Authority found in a 2018 survey that 70% of banks recognise climate change poses financial risks, but also showed that so far only 10% of institutions take a long-term strategic approach to manage these risks.

Experts in the market are in agreement that the full extent of climate change risks, be they of physical or transitional nature, are not yet fully understood. Further attention will be required from industry, academia and governments to improve data and methodologies to assess the potential impact of those risks on various regions or industries.

One of the main methodological challenges is the lack of historical data to assess potential impacts of shocks, which requires risk managers to make forward-looking assumptions and develop scenarios that are yet to be tested against reality. The goal of internalising external effects is challenging given quantification of the effects of environmental events in economic terms is rarely being undertaken.

In contrast to extreme weather events, on which in particular insurance companies have built up expertise and granular data, the more subtle costs and impacts on the economy by incremental changes to the climate are much less easily available because they are not usually assessed holistically. In order for climate change risk management to be effective on company level, such analyses on a macro level need to be enhanced in the future by academia or governments to enable incorporation into banks' and other financial institutions' risk assessments. Smart use of technology could significantly enhance such efforts, as would international cooperation.

Notwithstanding the challenges, financial institutions have started to work on establishing the use of scenario analysis and stress testing to stimulate, understand and quantify climate change risks to their balance sheets and business models in the short, medium and long term (see UNEP FI initiative described in Table 2).

Tackling climate change risks in the financial system: Industry and government initiatives

While individual banks' efforts to include climate change risks in their business considerations are important, the threats to financial stability have to be addressed from a more systemic perspective. A number of industry and government initiatives have been established to work on a common approach towards a climate-resilient financial system, focusing on increasing data availability and transparency, improving risk assessment methodologies, and establishing a better common understanding of what is 'green' and what is not.

Table 2: Overview of initiatives to tackle climate change risks

G20 Green Finance Study Group/ G20 Sustainable Finance Study Group	In 2016, the G20 launched a Green Finance Study Group (GFSG) under the lead of the Chinese Presidency, to investigate possibilities to encourage private investors to increase green investments. Under Argentina's Presidency in 2018, the G20 members adopted the work of the GFSG to the broader concept of sustainable finance, leading to the change of its name to the Sustainable Finance Study Group. Its latest synthesis report outlining voluntary options to support deployment of sustainable private capital has been formally welcomed by the G20 in July 2018.
FSB Taskforce on Climate-related Financial Disclosure (TCFD)	The industry-led Task Force on Climate-related Financial Disclosures (TCFD) set up by the FSB in 2016 released its final recommendations in June 2017 to provide a framework for companies to develop more effective climate-related financial disclosures through their existing reporting processes. A status report in 2018 showed that a majority of the 500+ companies supporting the principles disclose some climate-related information. However, financial implications are often not disclosed, and information on strategy resilience under different climate-related scenarios is limited, which indicates that it is still early days for overcoming the challenges of
Network for Greening the Financial System (NGFS)	In December 2017, eight central banks and supervisors established the Network of Central Banks and Supervisors for Greening the Financial System (NGFS). Since then, the NGFS has grown to currently 24 Members and 5 Observers across five continents. The network aims to strengthen the global response required to meet the goals of the Paris Agreement and to enhance the role of the financial system to manage risks and to mobilise capital for green and low-carbon investments in the broader context of environmentally sustainable development. In October 2018, the NGFS published a progress report on national, regional and international initiatives.

European Commission Sustainable Finance Action Plan	In March 2018, the European Commission released its Action Plan on Financing Sustainable Growth. The Action Plan is aimed at reorienting capital flows towards sustainable investment, mitigating the impacts of climate change and other environmental and social issues on the financial system, and increasing transparency and long-term finance. In May 2018, the Commission presented a series of measures to start implementing its Action Plan, including three legislative proposals (on disclosure requirements, low-carbon benchmark and the creation of a taxonomy). From March to July 2018, the Commission also conducted a consultation to assess the relevance of the EU framework addressing public reporting by companies.
UN Environment Finance Initiative (UNEP FI)/TCFD Pilot	In July 2018, sixteen banks convened by the UN Environment Finance Initiative (UNEP FI) released new methodologies to understand and manage physical risks and opportunities of climate change in loan portfolios, in line with recommendations of the TCFD. The methodologies were piloted across three climate-sensitive industry sectors: agriculture, energy and real estate, demonstrating the need for a balanced approach to assessing the risks to banks' clients and loan books from both incremental climate change (such as rising temperatures and changing precipitation patterns) and increasingly frequent and extreme weather events. The guidance also aims to inform banks' strategies to support clients in adapting to changing conditions.

Turning sustainable finance into an opportunity for more integrated financial markets

While the risks of climate change for the financial system are being addressed from a risk management and disclosure perspective, many of the initiatives described above do not only aim to strengthen the financial system's resilience to climate change risks, but also help fight climate change by reallocating investments towards climate-friendly alternatives, e.g. clean energy infrastructure. The market for green or in the wider sense sustainable financial products has significantly grown in the past years and represents a great opportunity for banks. Contrary to common beliefs, a much-cited 2015 meta study by Friede, Busch and Bassen across more than 2000 empirical studies found that there is a strong business case for sustainable investing. 90 percent of the studies analysed found that sustainable and impact investments can at least match the returns of ordinary investments. Judging by pledges made by asset owners, the future potential is even bigger: The Portfolio Decarbonization Coalition (PDC), which was set up in late 2014 aiming to mobilise a critical mass of institutional funds to drive decarbonization, currently counts member commitments of more than USD 600 billion for decarbonization investments. The Montreal Pledge, also launched in 2014, requires signatories to measure and publicly disclose the carbon footprint of investment portfolios on an annual basis, and has so far been signed by asset owners and fund managers with more than USD 10 trillion under management. All of this shows that realigning financial flows towards a low-carbon economy does not necessarily have to be brought about by strict regulatory measures and prescriptive rules. On the contrary, this is a market that shows great potential for innovation – in particular if it can be further unlocked by removing existing regulatory hurdles.

As an example, accessibility of sustainable investing products, including to combat climate change, could be improved.

Cross-border applicability of standards

The EU's efforts in the context of the Sustainable Finance Action Plan raises important questions. In particular a broadly supported taxonomy for sustainable products could be highly useful to investors to better understand and navigate the sustainable finance landscape. However, the benefits of developing a taxonomy that determines in a binary way which industries or activities (e.g. nuclear power, electric transport, agriculture intensification) are 'good' or 'green' and which are 'bad' or 'brown' are less clear at this point. Such a detailed taxonomy may be constraining and marginalise sustainable investing rather than improving its accessibility. Furthermore, there is a risk that an EU focused taxonomy and further rules derived from the EU action plan could further complicate market access and equivalence considerations. Such a taxonomy should be flexible enough to incentivise global applicability without hindering

market access or innovation in the area of sustainable finance. The same would apply to some of the other actions described in the plan, such as labelling.

Ensuring cross-border marketability of impact investing products

Within the sustainable finance space, arguably the most impact can be generated by investing in an earlier stage, sustainable businesses and private market funds. Such investments have a much larger part in driving the transition to a low-carbon economy than e.g. simply picking stocks based on sustainability criteria (unless accompanied by robust shareholder engagement). However, many of the most impactful products are not available to smaller investors due to investor protection rules and high thresholds for becoming a qualified investor.

While cross-border marketability – even within the EU – can be an issue for 'traditional' private market products, its effects on impact investing – which is still a small market – can be even more pronounced. Especially smaller venture capital, private equity and private debt funds may have difficulty growing to scale if obstacles to their global distribution are not overcome (e.g. AIFMD regulation, which creates significant overheads for small private market impact funds).

To ensure impact, products might need to be differently constructed than what is currently allowed for retail investors. Therefore, broadening investability, suitability and applicability is key.

The main difficulty lies in the trade-off between the investor protection rules that cause the hurdles, and the aim to improve financial asset allocation towards sustainable undertakings. The implications outlined above show that this comes at a cost, which is potentially disproportionate for niche products in the sustainable investing area. However, adjusting investor protection without incurring undue risks may prove to be a difficult balancing act.

Policymakers should look out for ways to improve accessibility and strengthen market mechanisms and infrastructure for people willing to invest money in climate change mitigation. Some learnings for adjustments may be derived from the different efforts related to regulation of Fintech investment platforms such as crowdfunding or peer-to-peer-lending.

Summary

There is a unique opportunity to make financial markets more integrated and more liquid, and sustainable investing products more commonly understood if regulators address some of the issues sustainable finance products currently face. These include a lack of a common understanding of definitions, cross-border marketability issues, as well as prohibitive investor protection rules, to name but a few. The past few years, in particular since the Paris Agreement in 2015, have shown significant activity. Banks are aware of issues related to climate change risks and are working to address them on an individual level, as well as with industry initiatives. The role of regulators should primarily be to remove unnecessary hurdles rather than issuing prescriptive rules that could be harmful to innovation in this fast-moving and promising field.

CHAPTER 3

KEY POLICY RECOMMENDATIONS

1. ACHIEVE COMPLETION OF PRUDENTIAL REFORMS, ASSESS THEIR IMPACT AND DEVELOP A FORWARD-LOOKING APPROACH FOR THE FUTURE

Updating the quantitative impact studies of past reforms to account for cumulative effects

The global financial crisis was rooted in a multiplicity of factors. Consequently, action taken at global level over the past ten years comprises individual measures aimed at addressing different shortcomings in the financial system. Each of these measures was targeted at a specific issue and is assessed against its individual impact on the financial system and the overall economy. However, correlations and cumulative effects exist among individual measures such as higher going and gone-concern capital requirements, enhanced margin requirements, CCP default fund contributions and bank resolution fund contributions. The impact of higher regulatory-induced operating and funding costs hampers not only the first buffer against losses before capital, but also limits banks' ability to continue investing in new technology and to better analyse and address evolving risks. Against this background, we suggest a move away from quantitative impact studies assessing only one set of regulatory requirements (e.g. Basel III) towards an approach which takes into account the cumulative effects of regulatory requirements on firms as outlined above.

Removing inconsistencies, outdated legislation and closing regulatory gaps

In 2015, the European Commission launched a Call for Evidence intended to screen 40 new pieces of EU legislation to restore financial stability and market confidence and to solicit feedback from stakeholders. The call sought to monitor the continuing development, implementation and functioning of the new rules in order to check that they were delivering as intended. It was aimed at making sure unintended consequences, inconsistencies and gaps in the current regulatory framework were addressed. Most respondents agreed that the reforms have enhanced the resilience of the financial system, but also identified examples of possible friction, overlap and other forms of unintended interaction between different rules. These findings are not only relevant at European level but also have a global dimension. Therefore, global standard setters should increase resources to assess the efficacy of historic reforms, as the volume of such assessments increases.[46]

Developing a new form of global regulatory dialogue

Last year our Discussion Paper focused on international regulatory cooperation to counter the risks of fragmentation.[47] We argued for improving the governance of the global standards-setting process by enhancing transparency, predictability and stakeholder's involvement, because actors who are closely and fairly involved in the setting of global standards will be more committed to applying agreed rules in a consistent manner. We support therefore the direction set by Randal Quarles in his inaugural speech as FSB Chairman. These arguments hold true and we continue to see the need for stronger and more formal involvement of the industry and of other relevant stakeholders. In addition, practical experience with the application of global standards by the industry can help identify shortcomings and possible improvements. Furthermore, there are a number of adverse consequences which will surface over coming years in particular as the monetary policy environment normalises, combined with the emergence of risks rooted outside the financial sector, but affecting it directly. All this needs to be analysed and addressed by regulators and politicians, through an open and fact-based debate among relevant stakeholders. For example, regulators should be more transparent in the methodology of their quantitative impact studies and seek to take account of market data with the support of firms. Further, more regular roundtables involving the private sector would help to inform policy decisions and set the basis for fully transparent conclusions. Regulators should also publicly consult with the full range of their stakeholders concerning their work programme to ensure relevance and appropriateness. Not only would such an approach reinforce public policies in targeting vulnerabilities, but this would also strengthen their credibility and the acceptance of a more consistent global implementation.

2. DELIVERING FINANCIAL STABILITY IN AN EFFICIENT MANNER

Ensuring consistent implementation, and avoiding excessive ring-fencing and fragmentation

Recent developments point to increasing national divergence from international standards, adding either new or conflicting rules motivated by a primarily domestic perspective on financial stability. Such approaches create inconsistencies that put the efforts of building a stronger financial system at risk. Fragmentation can indeed impair financial stability by reducing market liquidity and trapping scarce resources in domestic markets. The example of the globally agreed loss-absorption standard (TLAC) demonstrates that further improvements may be found when it comes to implementation at national level. Many jurisdictions, including the European Union, do not apply the flexibility enshrined in the TLAC standard as it was designed. Instead of allowing resolution authorities to attribute to banks a loss absorption that reflects their resolvability and capitalisation within the 75-90% range (as set out by the FSB), the EU's Risk Reduction Measures (CRR II) requires all third-country banks to hold internal loss absorption (internal TLAC) at a fixed percentage of 90%. Consequently, scarce resources are trapped at the level of individual entities and are not at the disposal of the group resolution authority in the event of a crisis. This increases the likelihood of bank failure and puts too much emphasis on loss absorption compared to other elements that are also key for efficient bank resolution.

Once started, the race to trap scarce resources in individual jurisdictions may not be stoppable and even accelerate the renationalisation of resilience measures. If this trend becomes entrenched, efforts made in the past ten years to establish a stable and sound global financial system will be eroded. We support an implementation of capital, liquidity and (internal) TLAC requirements in a way that does not trap resources locally but rather allows for sufficient fungibility of resources at group level to appropriately allocate capital where it is most needed. Local ring-fencing of resources to build up buffers might be a rational decision for an individual jurisdiction, but it actually increases risk in the overall system because there is less flexibility within firms to address issues using resources cross-border and to allocate capital and liquidity where it is most needed. To address these challenges and avoid a further escalation of the issue we call for a closer dialogue among authorities and with the industry, supported by a further formalization of cooperation agreements.

Improving the operationality of the agreed regulatory framework

The impact of global reforms should be carefully assessed to ensure they achieve their intended objectives and do not lead to unintended consequences or unnecessary complexity through design, cumulative effects or gaps leaving some risks unaddressed or new market entrants outside regulatory scope. Regulators should monitor implementation of reforms and consider together with key stakeholders whether amendments are made. In addition, regulators should consider, in collaboration with key stakeholders, where more guidance can be needed to fully operationalize agreed reforms. While global policies should remain principle-based, more directional guidance is needed in some areas to support national regulators in their implementation work. As an example, the absence in some jurisdictions of a public mechanism that provides for temporary funding in resolution considerably reduces the use of the best suited resolution scenario and should be corrected swiftly.

Extracting the benefits of new technology

Technology can help banks to be innovative, competitive and sustainable in the long-term, assuming they embrace technological change as an opportunity rather than a threat. Regulators will need to assist the industry by looking at ways to support the adoption of new technologies to facilitate the delivery of regulatory requirements. RegTech has enormous potential to enable better compliance solutions, increasing efficiency, profitability and to reduce entry barriers for the sector. Furthermore, financial institutions increasingly make use of machine-learning and advanced data analytics to help them in areas such as credit risk assessment and anti-money laundering/fraud detection checks. Regulation and supervisory practices should support banks in their efforts to drive innovation in this space and encourage technology-based regulatory compliance.

3. MOVE TO A NEW ENGAGEMENT MODEL TO BETTER PREPARE FOR EVOLVING RISKS

Reduce regulatory complexity

Arguably, financial innovation and the more than ever global scale of financial markets require new and more complex rules. Nevertheless, we see possibilities for reducing regulatory complexity without reducing financial stability and resilience. On the contrary, if rules become too complex, their correct application will be difficult to monitor and supervise and investors will find it hard to compare relevant bank data, thereby weakening market discipline. Well targeted simplification will increase market resilience and certainly not weaken it (see our first case study for specific recommendations). Simplification should start in areas where unintended consequences are evident. Regulatory complexity is a cross-cutting topic and is already addressed in some of the recommendations we make. First, reviewing and adapting the individual crisis-driven regulatory changes under the heading of creating a single coherent and consistent set of rules may allow for the elimination of overlaps and of sometimes contradictory provisions. Aiming at transposing global standards in a consistent manner and without national gold plating and/or national ring-fencing will allow global banks to implement and apply global solutions in risk management and IT. The regulatory review and assessment of financial regulation should be stepped up and an analysis of the trade-offs is necessary in order to strike the right balance between risk sensitivity, comparability and simplicity. Supervisory cooperation and convergence will help. A second issue is trust. Increasing trust among global supervisors and enhancing transparency concerning supervised entities may allow for more outcome-based rules instead of ruling each topic in a detailed and increasingly complex manner. Finally, if supported and promoted by regulation and supervisory practices, new technology can become a strong driver for managing and potentially reducing complexity in the area of reporting and compliance.

Take cybersecurity to the next level

The financial system has made progress in identifying issues and implementing measures to tackle cyber-risks. As we demonstrate in our second case study, there is a solid framework in place for the supranational governance of cybersecurity. This does, however, require further alignment and simplification as the characteristics and concentration of risk scenarios evolve and cyber-attacks gain in both magnitude and complexity. This in turn requires still stronger cooperation among regulators and between the public and private sectors (including with third countries) as well as international alignment of cybersecurity rules, regulations and practices. To be most effective, efforts should encompass people, governance, and technology. The scope should extend to third parties, including suppliers, partners, and clients. But just as with other complex financial regulation, cybersecurity regulation can become a burden on businesses unless applied with a high level of pragmatic consistency. In the area of intelligence and information sharing, for example, banks should explore synergies with each other and with governmental authorities, as well as across borders, to better identify new opportunities for prevention but also to protect shared infrastructures. Timely information sharing around cyber-threats and cyber-attacks is essential, so that the data can not only be used to protect customers, but also shared to protect the stability of the financial system. Existing barriers to effective information sharing should be addressed, primarily by reinforcing cross-border coordination amongst the various actors; and regulators should coordinate national frameworks. A second area for attention is corporate governance where cybersecurity strategy should be driven at Board level and integrated into firms' business strategy and risk management. A third area is achieving better regulatory consistency and coherence by taking into account the implications for cyber-risks and personal data protection when designing and/or reviewing regulations aiming at higher user convenience and consumer choice (such as the revised EU Payment Services Directive - PSDII). Such regulatory efforts should lead to the development of principle-based standards, globally aligned to avoid a fragmented regulatory landscape exploitable by cyber-attackers to disrupt the functioning of financial markets. Financial institutions and regulators should also collaborate to ensure proper financial education and increasing awareness about the need for protection of all users of digital financial services against fraud, identity theft and organised financial crime.

Need for close collaboration to address climate change risks

Addressing the complex issue of climate change risks in the financial system while equally embracing the opportunities for innovation in this area will require close collaboration between relevant players from governments, industry, and academia. The following three focus areas will need to be part of any effective and consistent response to the trend. First, removing regulatory hurdles: In the green and sustainable finance space, regulations that may harm innovation or reduce the reach of respective products need to be reviewed to see if they can be made more conducive to growth in this field (while not compromising on the core aim of the regulation). Such an outcome requires close dialogue between policymakers and the industry that is driving innovation in sustainable finance, including to combat climate change.
Second, consistent implementation: cross-border collaboration of regulatory authorities will be required to ensure the framework to address issues related to climate change in the financial system in a way that is as globally aligned and consistent as possible. For example, work on the European Commission Action Plan's taxonomy should be guided in a direction that allows the concept to become easily applicable in other countries. Standards related to the taxonomy must not further harm liquidity in and accessibility of sustainable investment markets across borders. Third, common understanding of climate change scenarios: Climate change risk management will increasingly require consistent macroeconomic data concerning potential impact scenarios for certain economies or industries. For comparability reasons such information would mostly have to be aggregated by governments and central banks together with academia (ideally supported by the smart use of technology).

ABBREVIATIONS

AIFMD	Alternative Investment Fund Managers Directive
AMA	Advanced Measurement Approach
API	Application Program Interface
BCBS	Basel Committee on Banking Supervision
BIS	Bank for International Settlements
CCP	Central Counterparty Clearing House
CET1	Common Equity Tier 1
CFTC	Commodity Futures Trading Commission (US)
CPMI	Committee on Payments and Market Infrastructure
CRO	Chief Risk Officer
DRR	Digital Regulatory Reporting
EBA	European Banking Authority
EBF	European Banking Federation
EC3	European Cybercrime Centre (Europol)
ECB	European Central Bank
ENISA	European Network and Information Security Agency
ESG	Environmental, Social and Governance
ESMA	European Securities and Markets Authority
EU	European Union
FATF	Financial Action Task Force (on Money Laundering)
FBO	Foreign Banking Organisation
FCA	Financial Conduct Authority (UK)
FMI	Financial Market Infrastructure
FSB	Financial Stability Board
G-SIB	Global Systemically Important Bank
GDPR	General Data Protection Regulation
GFSG	Green Finance Study Group
HQLA	High Quality Liquid Assets
ICT	Information and Communications Technology
IIF	International Institute of Finance
IMF	International Monetary Fund
IOSCO	International Organisation of Securities Commissions
IRB	Internal Ratings Based
ISDA	International Swaps and Derivatives Association
IoT	Internet of Things
J-CAT	Joint Cybercrime Action Taskforce (Europol)
LCR	Liquidity Coverage Ratio
MDA	Maximum Distributable Amount
MERR	Machine-Executable Regulatory Reporting
MiFID/MiFIR	Markets in Financial Instruments Directive/Regulation
MREL	Minimum Requirement for own funds and Eligible Liabilities
NATO	North Atlantic Treaty Organisation
NGFS	Network for Greening the Financial System
NGO	Non-Governmental Organisation
OECD	Organisation for Economic Cooperation and Development
OTC	Over-the-Counter
PDC	Portfolio Decarbonization Coalition
PSD	Payment Services Directive
RRP	Recovery and Resolution Plan
RWA	Risk Weighted Assets
SRB	Single Resolution Board
SSM	Single Supervisory Mechanism
TBTF	Too-Big-to-Fail
TCFD	Taskforce on Climate-related Financial Disclosures (FSB)
TIBER	Threat Intelligence-based Ethical Red Teaming (ECB)
TLAC	Total Loss Absorption Capacity
UCITS	Undertakings for the Collective Investments in Transferable Securities
UNEP FI	United Nations Environment Programme - Finance Initiative
UK	United Kingdom
WEF	World Economic Forum

ENDNOTES

1 BIS, *Annual Economic Report*, June 2018.

2 McKinsey Global Institute, *A decade after the global financial crisis*, September 2018.

3 McKinsey Global Institute, *A decade after the global financial crisis*, September 2018.

4 Axel Weber, *The impact of financial regulation: A G-SIB perspective*, Banque de France, Financial Stability Review, April 2017.

5 Basel Committee on Banking Supervision, *Basel III Monitoring Report*, December 2017.

6 Speech by Stefan Ingves, Chairman of the Basel Committee on Banking Supervision, *Basel III are we done now?*, Frankfurt, 29 January 2018.

7 Benoit Coeuré, *Central clearing: reaping the benefits, controlling the risks*, Financial Stability Review, April 2017.

8 G 20 Leaders' Statement, the Pittsburgh Summit, September 24-25, 2009.

9 FSB 2018 Resolution Report, *'Keeping the pressure up'* Financial Stability Board, *Seventh Report on the Implementation of Resolution Reforms*, 15 November 2018.

10 FSB, *Seventh Report on the Implementation of Resolution Reforms*, 15 November 2018.

11 OECD Steering Group on Corporate Governance, *The Corporate Governance Lessons from the Financial Crisis*, Paris 2009.

12 BCBS, Progress in adopting the *'Principles for effective risk data aggregation and risk reporting'*, June 2018.

13 FSB, *Supplementary Guidance to the FSB Principles and Standards on Sound Compensation Practices*, March 2018.

14 G 20 Leader's Statement, the Pittsburgh Summit, September 24 – 25 2009.

15 Speech by Ryozo Himino, Vice minister for international affairs, FSA, Japan, at the 2018 ISDA Annual Japan Conference, Tokyo, October 26 2018.

16 D. Wilson Ervin, *The Risky Business of Ring-Fencing*, December 2017.

17 Elke König, *Gaps in the Banking Union regarding funding in resolution and how to solve them*, Eurofi, September 2018.

18 Randal K Quarles, *Vice Chairman of the Board of Governors of the Federal Reserve System and Chair of the Financial Stability Board: Ideas of order – charting a course for the Financial Stability Board*; speech delivered on 10 February 2019, Hong Kong.

19 FSB work programme for 2019, 12 February, 2019.

20 Speech by Pentti Hakkarainen, Member of the Supervisory Board of the ECB at the Lisbon Research Centre on Regulation and Supervision of the Financial Sector Conference, Lisbon 6 June 2018.

21 World Economic Forum, *Regional Risks for Doing Business 2018*, Insight Report.

22 Interview of ECB Executive Board Member Benoît Coeuré with Der Tagesspiegel, 1 October 2018.

23 Bank of England, *FCA Joint Discussion Paper on Building the UK financial sector's operational resilience*, July 2018.

24 2018 Resolution Plan Agency Feedback.

25 BIS, *FSI Insights on policy implementation No 2: Regulatory approaches to enhance banks' cybersecurity frameworks*, 2017.

26 Accenture, *Cost of Cyber Crime*, 2018.

27 IMF Working Paper WP/18/143, *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment.*

28 BIS, *FSI Insights on policy implementation No 2: Regulatory approaches to enhance banks' cybersecurity frameworks*, 2017.

29 *Cyber Security in Securities Markets – An International Perspective Report on IOSCO's cyber risk coordination efforts,* 2016.

30 IBM, *2018 IBM X-Force Threat Intelligence Index*, 2018.

31 World Bank Group, *Financial Sector's Cybersecurity: A Regulatory Digest*, 2017.

32 Press announcement, *FSB publishes stocktake on cybersecurity regulatory and supervisory practices*, 13 October 2017.

33 EU Communication, *Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry*, 2016.

34 *G7 Principles and Actions on Cyber.*

35 *Global guidance on cyber resilience for financial market infrastructures.*

36 *CPMI-IOSCO release guidance on cyber resilience for financial market infrastructures*, 29 June 2016.

37 FSB, *Cyber Lexicon Consultative Document.*

38 EBA, *Guidelines on ICT Risk Assessment under the SREP*

39 *Joint committee report on Risks and vulnerabilities in the EU financial system*, April 2018 (JC 2018 07).

40 *Mandate of the Euro Cyber Resilience Board for pan-European Financial Infrastructures*, 26 January 2018.

41 *National Cybersecurity Strategy Guide.*

42 IIF, *Fighting Back Against a Cybersecurity Attack*, 2015.

43 IIF, *Addressing Regulatory Fragmentation to Support a Cyber-Resilient Global Financial Services Industry*, 2018.

44 Mark Carney, *Breaking the tragedy of the horizon – climate change and financial stability*, Lloyds of London, 29 September 2015. https://www.bis.org/review/r151009a.pdf.

45 Others have since subsumed liability risk under transition risks rather than as a separate category.

46 Remarks by FSB Chair Randal K. Quarles, 10 February 2019: http://www.fsb.org/wp-content/uploads/Quarles-Ideas-of-order-Charting-a-course-for-the-Financial-Stability-Board.pdf.

47 https://www.swissfinancecouncil.org/images/pdf/SFC_Discussion_Paper_2018.pdf.

SwissFinanceCouncil

Fostering International Dialogue

Swiss Finance Council
EU Representative Office
Square de Meeûs 23, B-1000 Brussels
T +32 2 430 37 00
www.swissfinancecouncil.org