

Systems of Cyber Resilience: Secure and Trusted FinTech

July 2020



World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744
Email: contact@weforum.org
www.weforum.org

© 2020 World Economic Forum.
All rights reserved. No part of this
publication may be reproduced or
transmitted in any form or by any
means, including photocopying and
recording, or by any information storage
and retrieval system.

Contents

Preface	4
Introduction: World Economic Forum FinTech Cybersecurity Consortium	6
1. Executive Summary	7
2. Systems of cyber resilience: building cyber-resilient controls for the financial (eco)system	10
3. Creating a system of resilience: universal cybersecurity controls and assessment	13
4. Approach	14
5. Criteria for choosing base-level frameworks	15
6. Candidate frameworks	18
7. Center for Internet Security Top 20 Critical Security Controls	19
8. The Financial Services Cybersecurity Profile	21
9. Conclusion	25
10. Appendix 1: The CIS CSC 20 vs. base-level controls criteria	26
11. Appendix 2: The FSC Profile vs. base-level controls criteria	30
12. Appendix 3: The role of industry and public-private initiatives	32
Contributors	33
Endnotes	34

Preface



Matthew Blake

Head, Platform for Shaping
the Future of Financial and
Monetary Systems



Daniel Dobrygowski

Head of Corporate
Governance and
Digital Trust, World
Economic Forum



Adrienne Allen

Director of Security GRC
and Privacy, Coinbase

Cyber risk is pervasive, systemic and global in scope. In the financial services industry, it is increasingly difficult to mitigate this risk, since the modularization of financial services interlinks organizations whose cybersecurity maturity levels vary greatly. It is therefore difficult for any one firm to understand how an attacker might move laterally across a supply chain. Given that interests and priorities diverge among actors, a sector-wide baseline for cybersecurity is necessary to ensure the integrity of the global financial system. A vital step in establishing this baseline is for financial technology (FinTech) companies to uphold their obligations to system resilience. FinTech companies must protect themselves and their customers in a measurable and demonstrable way, but they are often faced with fragmented regulations and finite resources, and operate in a market where skilled expertise is in short supply. This Consortium helps raise the level of FinTech cybersecurity by supporting the scaling and adoption of frameworks that provide clear and achievable cybersecurity guidelines to FinTechs to enhance the security of the wider financial services supply chain. More significantly, this work is a vital step towards creating durable partnerships that will improve the cybersecurity and resilience of the global financial system. Additional organizations - including the Cyber Risk Institute, supported by the World Economic Forum, and the Coalition to Reduce Cyber Risk – will carry this group’s recommendations forward to implementation across the financial sector globally.

Coinbase

Large multinational financial services organizations and FinTechs have a unique partnership. They provide services to each other and to similar customers, communicate with the same regulators, and as a result have highly interconnected cyber risks. That said, there are also significant variances across third-party due diligence approaches and prioritization of cyber-risk management activities. This can make compliance with third-party diligence requirements or financial regulatory requirements impractical and cost prohibitive for FinTechs. The FinTech Cybersecurity Consortium addressed this challenge by providing a collaborative forum to assess existing cyber-risk frameworks and converge on an “on-ramp” that allows FinTechs to achieve a baseline risk posture. This recommendation is an exciting endorsement that frees FinTechs to focus their resources on the highest-impact activities that help achieve the baseline and effectively communicate risk maturity.



Adam Sommer
Vice-President, Industry
Standards at Mastercard

Mastercard

FinTechs play an important role in the digital transformation that makes our lives simpler, more convenient and rewarding. For FinTechs to scale sustainably, collective partnership is required. However, FinTechs cannot achieve impact and scale without proper cyber protocols. Collaboration is critical – sharing expertise, defining standards and playing a leading role in securing the landscape. The FinTech Cybersecurity Consortium enables FinTechs to innovate responsibly, protect the digital ecosystem, align security with consumer experience and reduce risk. At Mastercard, safety and security are foundational principles for every part of our business and the technology platforms and services we enable. As our digital landscape expands along with our dependence on it, our expectations of cybersecurity need to be continuously considered and refined. Cybersecurity must never be an afterthought.



Jim Maloney
Chief Security and Privacy
Officer, Social Finance (SoFi),
World Economic Forum
Expert Network member

SoFi

FinTechs can be a valuable source of innovation for the financial services industry, but only if those innovations can be delivered with security controls that meet industry and regulatory requirements. The effort described in this document aims to provide FinTechs with guidance that can put them on a path towards a robust security programme that can be applied in the earliest stages of the business. As both a provider and consumer of technology focused on financial services, SoFi has found the approach described herein to be a key enabler for participating in this critical industry sector.



Sunil Seshadri
Senior Vice-President,
Chief Information Security
Officer, Visa

Visa

Fintech innovations deliver tremendous economic and social benefits, connecting unbanked and underbanked populations to the digital economy, contributing to small business growth, and empowering consumers in new and exciting ways. As larger financial service organizations increasingly look to partner with FinTechs, gaps between the security capabilities of established firms and young FinTechs can present real challenges to collaboration. At Visa, our commitment to security is unwavering. This includes our responsibility to help secure the wider payments ecosystem by encouraging best practices and sharing relevant insights. The work of the World Economic Forum's FinTech Cybersecurity Consortium will provide valuable first steps to help new companies develop secure, market-ready solutions.

Introduction: The World Economic Forum FinTech Cybersecurity Consortium

The FinTech Cybersecurity Consortium formed in 2018. Its aim was to facilitate the reasonable protection of a dynamic and growing global Financial ecosystem composed of established organizations with high levels of cybersecurity maturity and FinTechs rapidly developing and providing emerging technologies.

The security requirements of each participant in the Financial System vary, sitting along a continuum dependent on the countries in which a firm operates, the services it provides, the customers it targets and its impact on other participants in the market. This has made it difficult to provide smaller firms with guidance to weave cyber-resilience into their business and growth plans.







Consortium members asked, how can less mature FinTech companies connect with very mature organisations while maintaining a level of cybersecurity risk that is understood by all parties, accepted and manageable?

The Consortium believes that the security of the wider financial system requires the acceleration of FinTechs' access to methodologies for identifying cybersecurity risks and applying the practical steps needed to mitigate them. These methodologies should be scalable, by which we mean that they can be applied across borders so that a FinTech can use recognised cybersecurity best practice to facilitate entry to new markets and grow securely as it expands.

The FinTech Cybersecurity Consortium identified the simplification of baseline cybersecurity requirements for FinTechs as an important starting point. The Consortium has identified criteria for common minimum cybersecurity standards and controls that will obtain agreement from globally systemic financial institutions, FinTechs, governments and key regulators.

The Consortium's recommendations support the scaling and adoption of frameworks that provide clear and actionable cybersecurity guidelines to FinTechs to enhance the security of the wider financial services supply chain.

Figure 1 – Benefits of a cybersecurity controls framework for the entire financial ecosystem

 FINTechs	 INCUMBENTS	 REGULATORS	 CONSUMERS	 VCs	 TALENT
Understanding of what the bar is	Ability to partner	Streamlines/allows for more effective oversight	Protected from themselves	Streamlines due diligence	Ability to move across actors and jurisdictions
Avoidance of technical debt build-up	Accelerate innovation (cannot do it fast enough themselves)	Education	Confidence about security of information		
Consistency of language			Access to services		
Consistency across the value chain and mutual recognition					
	Improved efficiency				
	Streamlines due diligence				

A common framework to ensure a win-win-win-win-win-win outcome, involving understanding and articulation of benefits

1. Executive summary

1.1 Systems of cyber resilience: FinTech security controls and assessment

The World Economic Forum's Global Risks Report 2020¹ again named cyber threats as among the most significant risks to society and the economy in terms of likelihood and impact. The financial services sector remains a favoured and high-value target for cyberattacks.

Financial Services are becoming more modular and distributed, with many parties involved in service provision. This is usually to the benefit of consumers, but it has greatly expanded the number of targets available to cyberattackers.

Client data and assets are now spread across multiple platforms and providers. Risk levels, security requirements and security capability vary from organization to organization.

This medley of requirements leaves the sector in need of a mutually understood and widely accepted base level of cybersecurity controls. Clarity at the base level of security will support the effective protection of business and client assets across the wider supply chain. This will facilitate good cyber hygiene and cybersecurity techniques among the least resourced companies in the market, improving cyber resilience across the financial system.

Effective cybersecurity reduces the impact of cyberattacks on commercial operations, lowers the frequency and level of loss to clients and is essential to maintaining consumer trust in the wider financial system.

1.2 FinTechs

Financial technology (FinTech) companies are a vital source of accelerated innovation-driven improvements for the financial services industry.

Established financial services providers would like to partner swiftly and securely with innovative new FinTechs. This intention is shared by regulators and central banks, who see commercial links between new entrants and established providers as a benefit to citizens and the wider economy. FinTechs want strong commercial partnerships in order to survive and thrive.

However, the modularization of financial services interlinks organizations whose cybersecurity maturity levels vary greatly. This complicates cybersecurity risk management.

There are many approaches that FinTechs can take to make themselves cybersecure. Yet it is not always clear which control frameworks allow a FinTech to secure its assets, create trusted commercial partnerships with established firms and ensure compliance with relevant regulations in the jurisdictions in which it operates.

Established financial services providers have a number of frameworks, standards and industry-driven initiatives against which they can test the security of FinTechs and other third parties. However, the volume of industry initiatives, driven by the pace of technological change and the multiplication of regulations, is now creating "noise", which makes it difficult for FinTechs to direct their resources in a way that allows for security while facilitating the maximal number of commercial partnerships.

It is often the case that these cybersecurity standards and frameworks aim to achieve the same security objectives and vary mostly in their form and language. This leads to inefficiencies for both FinTech and established firms, which need to demonstrate compliance with regulations that vary slightly in form from jurisdiction to jurisdiction, but which have largely common objectives.

1.3 Incentivize security

The commercial incentive matters for security. Building a robust cybersecurity architecture is important for new-to-market organizations that depend on deterring even one cyberbreach to maintain business credibility. However, this can be expensive to deploy, take a significant amount of time to complete and can leave a firm hostage to early decisions on cybersecurity as it continues to grow.

As FinTech founders tend to balance a number of business needs, they may not necessarily prioritize security considerations in their product and services development.

This can lead to security-related technical debt that is difficult and expensive to address at a later date.

If information security teams are given the tools to clearly explain how their actions protect business assets and facilitate commercial partnerships, the executive team is more likely to understand and prioritize security, making it a core part of their firm's business growth plans. Implementation of cybersecurity controls is also likely to be more appropriate to the needs of each specific business and consequently more effective.

1.4 The challenge: fragmentation

FinTechs are entering the financial system at a time when governmental authorities have yet to coordinate and harmonize the development of rules and regulations across borders, even though the cyber threat is an internationalized one.

At the same time, financial services are becoming ever more specialized, causing industry to fragment into sub-sectors that set their own advice on security standards and implementation. Established companies are tailoring their due diligence requirements in order to better protect themselves and their clients.

The lack of coherence across the private sector as to which baseline standards FinTechs should implement, how they should be implemented and how this should be evidenced makes it difficult for FinTechs to apply their resources in a rational manner.

Rightly, nobody wishes to compromise on cybersecurity standards. All recognize that the current level of variation and duplication of requirements is unsustainable, pushing up the cost of compliance without always enhancing operational security.



1.5 Building on strong foundations

When it was set up in 2018, the FinTech Cybersecurity Consortium aimed to simplify baseline cybersecurity requirements for FinTechs by establishing the criteria for common minimum cybersecurity standards and controls. These criteria would be applicable across all market activities and, in tandem with assessment criteria, would enable a route to more specialized security depending on the services being provided.

This did not envisage the creation of a new standard. The Consortium entered a market in which there was much good work to build on. There are already several widely accepted cybersecurity standards,² a growing number of regulations with cross-border implications,³ guidelines,⁴ capacity-building toolkits,⁵ assessment certifications⁶ and cross-industry efforts to simplify or more efficiently manage the burden this creates for established firms and new market entrants alike.⁷ The desired approach was to review, adopt and enhance a few highly “portable” standards, as opposed to developing yet another standard.

These efforts all have value, but the volume of activity tells its own story. Despite efforts to simplify it, cybersecurity is inherently complex. There is a natural divergence between the

requirements of companies based on the services they provide, their size, resources and cybersecurity maturity level. Consequently, there is no silver bullet of perfect and ever-relevant guidance that FinTechs might follow.

Nonetheless, Consortium members saw the possibility of identifying a baseline set of security controls that would be common across all FinTechs, defining basic cybersecurity “hygiene” and providing meaningful reductions in cybersecurity risk.

Through its work, the Consortium concluded that simplifying and rationalizing existing standards is not enough. Providing advice on how to implement specific controls, though something to be welcomed by many FinTechs, is necessary but also insufficient as priorities will vary depending on the services provided by each FinTech and its position in the wider financial services ecosystem.

FinTech companies need to protect themselves in a measurable and demonstrable way. Adding to the challenge, they need to do this with limited resources and in a market where skilled expertise is in short supply.

2. Systems of cyber resilience: building cyber-resilient controls for the financial (eco)system

2.1 Recommendations:

- Expertise from industry, government and the non-profit sector should feed into the design of a future security management system that will incorporate controls frameworks, assessment processes, metrics and mapping of controls to financial services regulation.
- Control frameworks should be regularly updated so that they can mature with evolutions in the cyber-risk, threat and compliance landscapes
- In order to be applicable to FinTechs, these frameworks should be built with reference to guidance from international financial bodies and nation-state financial services regulations, emphasizing the regulations set in global financial services hubs so that they can be applied to as many markets as possible.
- Where financial regulators identify industry efforts that improve cyber resilience across the system, we recommend that they publicly endorse these initiatives in order to improve the chances of their adoption.

Financial and monetary systems are the cornerstone of economic activity. Over the past decade, important steps have been taken to strengthen the systems' resilience to external shocks. This includes steps to lower the impact of cyberattacks on operational resilience and maintain consumer trust in the safety of their assets.

Improving cyber resilience across the financial system has been complicated by accelerating technological disruption. This has put public institutions under pressure to demonstrate that

they are protecting consumers through regulation while also requiring the diffusion of some responsibilities down to industry groups.

In these circumstances, how can governments regulate and examine cyber risk in a way that is proportional, effective and does not create unwanted barriers to market entry? Where should responsibility sit for the development of granular cybersecurity controls and how should industry and the public sector engage with each other in this area?



2.2 The regulatory ecosystem



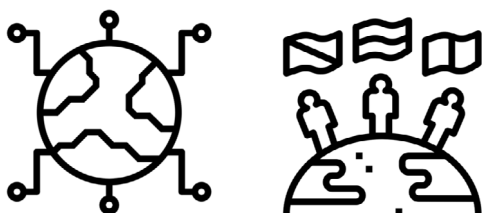
A number of international bodies set the tone for the global governance of cyber risk in the financial system. The Bank of International Settlements, Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions (CPMI-IOSCO), the Financial Stability Board, the International Monetary Fund and the World Bank all play a role.

For developing states, organizations such as the Alliance for Financial Inclusion, which brings together central banks, financial regulators and supervisors, supports its members in contributing to the development of global best practice and then adapting it to the particularities of each jurisdiction's environment.⁸

In some regions, supranational bodies, such as the European Central Bank, provide a degree of common shape to the governance of cyber risk.⁹

However, most rules are set at the level of the nation state and each nation-state authority responds to the specific needs of its jurisdiction.

2.3 Rules are local, but financial services, and the threats against it, are global



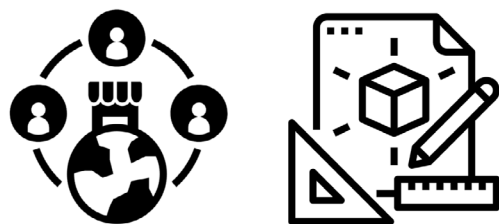
Regulations are usually set in the nation state, and compliance examined at the same level. This is straightforward for a FinTech operating in only one jurisdiction but, as FinTechs grow, they will often need to consider cross-border regulatory requirements.

Financial services and the cyberthreats against them are globalized. Countries' central banks and financial services regulators are often ill-equipped to address the complexities of these

cross-border threats, which evolve at a pace that policy development cannot match. It is nearly impossible to adapt requirements quickly enough to stay ahead of the technological changes harnessed by legitimate service providers and the attackers that wish to disrupt them. Responding through regulation runs the risk of creating a drag on private-sector cybersecurity efforts, where the level of security investment is high, response times are quicker and most expertise is housed.

As in other highly globalized services, such as the aviation sector, many financial services authorities have approached this challenge by concentrating their efforts on guidance resources for companies and governance structures for managing risk across the sector rather than regulations. This approach provides frameworks and best practices for companies but maintains space for industry to innovatively manage cyber risks.¹⁰

2.4 Cybersecurity controls that are market-defined but government-enforced



Cybersecurity controls require regular adaptation as technology, threats and business models change. While control objectives

may remain fairly stable (e.g. protect the confidentiality, integrity and availability of data and systems), the implementation of controls to meet those objectives are granular, specific to the assets they are meant to protect, and may have a limited shelf life.

There is a shortage of cybersecurity expertise globally and the private sector has acquired much of what exists. Government authorities can access expertise, and are responsible for training many experts, but resources are limited

and many authorities have taken the view that the development of granular controls is of less interest to them than the ability to understand whether the controls used by industry are effective and properly applied.

This dynamic certainly holds in the FinTech industry. Many companies possess an understanding of how to build, adapt and assess controls to protect them, and the experience of adapting controls and assessment to meet a multiplicity of slightly varying national regulations also sits largely in the private sector.

Consequently, we recommend that cybersecurity controls should be defined by financial services providers in consultation with cybersecurity experts from other sectors, governmental agencies and relevant civil-society organizations.

Efforts to build a more effective approach to cybersecurity controls will struggle to succeed if they fail to reflect the requirements of key regulators or cannot obtain a degree of regulatory support. Any standards adopted by the private sector will benefit from being examinable by financial services supervisors.

2.5 De-fragmentation

Cybersecurity regulations for the financial sector are fragmented across nation-state boundaries. As they continue to proliferate without alignment, it is becoming increasingly difficult for industry to design controls that have wide application and allow for new FinTechs to grow smoothly, securely and across borders.

Adopting a single, global, industry-wide baseline standard will create the efficiencies required to improve and encourage cybersecurity, especially in low-maturity FinTech firms. An approach to building an acceptable cybersecurity baseline for FinTechs, on which more specific requirements can then be added as a firm grows or specializes, is discussed in later sections.

3. Creating a system of resilience: universal cybersecurity controls and assessment

3.1 Recommendations:

- A common cybersecurity framework and assessment process is needed for low-maturity FinTechs.
- This should be tiered for cyber-security maturity levels and provide guidance for companies, as they grow, on when they need to adopt and enhance cybersecurity controls.
- The solution should start with baseline requirements for controls and assessment but provide an increasing complexity of controls as organizations develop and their cybersecurity risk-management requirements mature.



4. Approach

This section is based on findings from a series of workshops and events run by the World Economic Forum in 2018–2019.¹¹

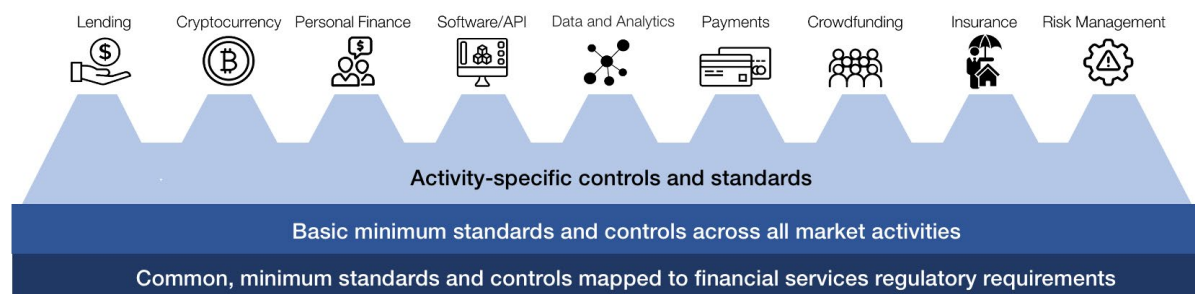
Members of the Forum's FinTech Cybersecurity Consortium argued for the creation and adoption of baseline security controls that could be applied to nearly every firm in the financial services ecosystem. These would then be combined with higher-level security controls relevant to a firm according to its offerings and place in the ecosystem.

This should account for variation arising from cybersecurity maturity levels, service offerings and location. Location, in particular, can affect both regulatory requirements and the threat landscape.

When discussing the scope of the framework to be developed, the working group determined that cybersecurity controls can be approached in tiers, similar to a certain Swiss chocolate bar. The first tier, the base of the chocolate bar, contains security essentials applicable to all financial technology companies, regardless of their business model.

The triangular peaks then represent specific requirements that depend on the business in which a company is active (e.g. payments or lending). FinTechs need to identify any industry-specific requirements and ensure these are incorporated in their security management system (an example of this would be the Payment Card Industry Data Security Standards [PCI DSS] requirements).¹²

Figure 2 – The tiered approach to cybersecurity controls



5. Criteria for choosing base-level frameworks

When developing the bottom layer of the chocolate bar, the members of the Forum's FinTech Cybersecurity Consortium developed

criteria to identify high-potential sources for baseline security controls. These criteria were informed by the considerations below.

5.1 Considerations in developing criteria for controls and assessment frameworks

When building criteria for base-level control frameworks, the Forum's FinTech Cybersecurity Consortium noted that challenges to creating cybersecure commercial partnerships range across technology, regulatory oversight, expertise and metrics, and also affect collaboration, as highlighted in the previous white paper, *Innovation-Driven Cyber-Risk to Customer Data in Financial Services*.¹³

When looking at a starting point for FinTechs hoping to apply cybersecurity controls and assessments, what needs to be considered? What factors should a controls framework account for?

Variation in needs

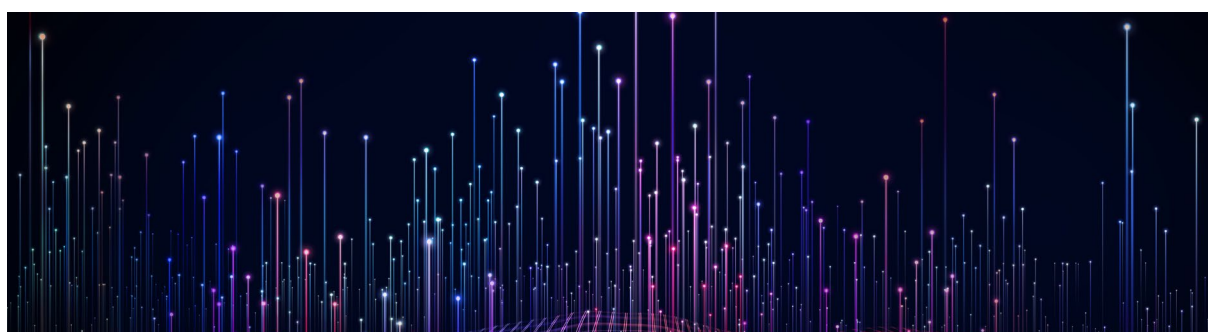
Cybersecurity requirements are not fixed. At the Cybersecurity Consortium Working Group's discussions in 2018–2019,¹⁴ a recurring theme was that cybersecurity requirements will vary for FinTechs based on maturity, jurisdictions served, services offered and the changing nature of cyberattacks over time. FinTechs need to understand what security requirements fit their specific circumstances now, as well as the steps they need to take for the future as they expand and grow.

Risk management priorities can diverge...

Young companies with limited service offerings and resources adopt cybersecurity standards only as needed to meet compliance obligations or to address well-known industry-level threats. Adoption tends to reflect these companies' growth paths and threat perception. Different FinTechs have very different starting points in terms of their understanding of cybersecurity and the compliance requirements of prospective incumbent partners.

...and converge

Established financial services providers and FinTechs have different perspectives on risk and risk management. However, they generally share the cybersecurity-related tenets of confidentiality, integrity and availability of customer data, and company data as a means for business optimization, business continuity and consumer protection. These common objectives apply to data at the highest level, as an ultimate objective for an effective cybersecurity programme, cascading down to applications, systems and networks.



Regulatory oversight

Even when a FinTech is not directly subject to regulatory oversight, it is likely to be supplying services to regulated entities. Every FinTech will have some regulatory footprint, which it will need to consider before it can enter the market. These requirements should be captured and understood early in the product life cycle.

Because security needs are influenced by so many factors, it is difficult to develop a one-size-fits-all approach that goes beyond baseline measures. It also suggests that an adaptable, business-driven and threat-based approach to controls is preferred to a more static capability-driven approach.

Assessing controls and measuring their impact on the business

Information security teams in FinTechs need to understand what their organization does and for what purpose when they start to develop their resilience plans. This sounds obvious, but many firms, not just those in financial services, have placed information security teams in an isolated position, making it difficult for them to understand the business value of the assets they are asked to protect.

Control metrics and systems of corporate governance that spread responsibility for cybersecurity risk management across an organization will support collaboration between information security and business teams. This then helps organizations prioritize the assets they need to protect, implement appropriate cybersecurity controls and demonstrate to potential commercial partners that they are managing cybersecurity risks at an acceptable and appropriate level.

Return on investment

Building a robust security programme – important for organizations that depend on deterring even a single cyberbreach in order to maintain business credibility – can be very costly to deploy and can take a significant amount of time to complete.

Return on investment is an important incentive for cyber-security best practice, particularly in growing companies for whom resources may be scarce. Smaller FinTechs should see clear

benefits when they apply resources to identifying and implementing the most effective security controls. If niche FinTechs are more secure, these FinTechs' commercial partners are more secure.

As FinTech founders balance a number of business needs, they may not prioritize security considerations in their product development. An effective assessment framework can instil a sense of urgency, as IT security teams can put clear risk data in front of senior decision-makers and show how cybersecurity risk affects the commercial viability of a product.

FinTechs need to know that allocating budgets to cybersecurity will not only make them more secure but also enable them to be seen by potential commercial partners as sufficiently secure to work with.

An effective risk-based controls framework begins with a route to a satisfactory security posture but it should help a FinTech demonstrate adequate security maturity to a prospective client or partner, particularly where that partner is subject to regulatory oversight.

Cyber resilience across the supply chain

A FinTech can test the cyber resilience of a product it provides, but this will have limited value if the organization acquiring that product does not also stress test the dependencies the product creates for them. For example, a FinTech might need to demonstrate redundancy planning to avoid downtime during the most likely scenarios of cyberattack; the organization purchasing the product would need to test its own ability to respond if the FinTech suffered a serious outage of service.

Financial institutions are highly interlinked. An understanding of an organization's role in the wider financial services ecosystem should be incorporated into its cybersecurity resilience planning. Planning for and conducting business continuity and resilience exercises, including the identification of third-party risks,¹⁵ is a shared responsibility between FinTechs and established financial services providers.¹⁶ Shared responsibilities are easier to manage if based on a common standard accepted by established firms and FinTechs alike.¹⁷

Framework proliferation

The proliferation of cybersecurity frameworks and regulations makes it difficult for some FinTechs to understand where to start and what the consequences of their choices might be for future commercial partnerships, cross-border growth or technical debt. Smaller FinTechs may find it challenging to determine an effective approach to evaluate and improve their cybersecurity readiness. This also affects established financial services providers, who may wish to partner with them.

A global standard for FinTech cybersecurity becomes necessary to enable partnerships and would equally benefit young technology companies, providing a measure of what level of security to aim for.

Base-level security controls – a common thread that allows for tailored solutions



There is a tension between the trend of modularization of financial services and the system-wide benefits of creating a universally applicable

set of baseline security controls with a common means of assessment.

At more advanced levels, financial services providers do require a tailored approach to the design of security controls. However, if a FinTech is tailoring all of its controls, then its business partners can tailor all of their requirements, and this greatly lowers the return on investment in security controls as it limits the number of commercial partnerships they provide. Many products, services and companies are unique, but the base-level controls needed to secure IT assets need not be.

5.2 Criteria for baseline cybersecurity control frameworks

The considerations above led to the creation of particular criteria:



- **Applicable anywhere:** Applicable in multiple jurisdictions – an effective baseline framework should be applicable in any jurisdiction, either because the controls are generic to multiple sectors or because they take account of regulatory requirements in the world's primary financial services hubs.



- **Controls map to commonly accepted cybersecurity standards and financial services regulation:** The framework clearly maps common information security standards, industry standards and relevant regulatory requirements to the controls it contains.



- **Tiered to maturity level:** The framework should be tiered to the size and maturity of an organization, creating a clear pathway towards ever more sophisticated controls as the need for them arises.



- **Prioritized:** Controls are prioritized or the framework supports FinTechs in assessing how to prioritize the implementation of controls in their organization.



- **Implementation tools:** The framework’s curators have developed or are developing tools that support FinTechs in evidencing the implementation of controls and measuring their effectiveness.



- **Self-assessment:** A self-assessment model is built around the framework.



- **Peer-to-peer comparison:** The framework’s curators provide data that allows FinTechs to understand their position in relation to their peers. This encourages underperforming firms to invest in cybersecurity.



- **Regular update cycles:** Framework curators have a clear programme for enhancing and updating controls and tools over time.



- **Potential for external validation:** The model links to a third-party assessment or audit programme that verifies the self-assessment and facilitates partnering between FinTechs and established financial services providers.



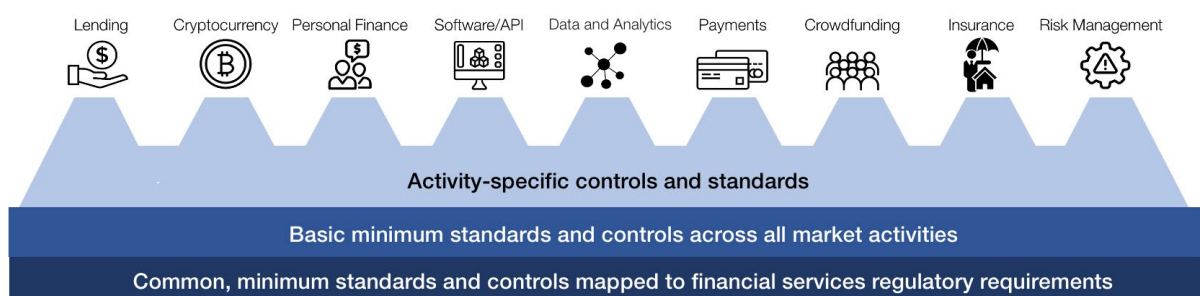
- **Scalable:** The framework has the potential for scaling, including indications of support from major financial services regulators, central banks or international organizations with responsibility for safeguarding the resilience of the financial system.

6. Candidate frameworks

Based on the criteria above, the Consortium focused on the Center for Internet Security Top 20 Critical Security Controls (CIS CSC 20) and the Financial Services Cybersecurity Profile (FSC Profile)¹⁸ for baseline security controls.

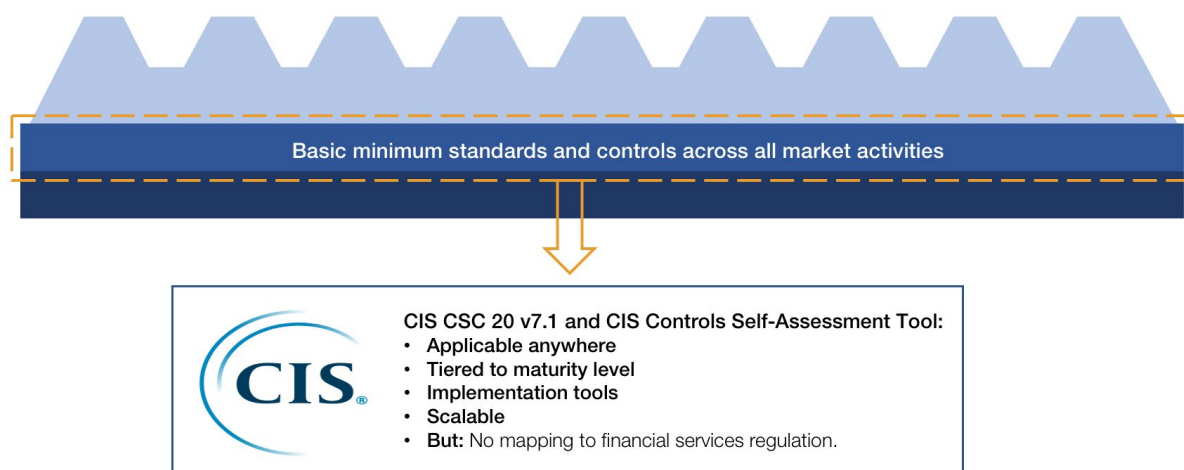
A detailed comparison of these frameworks against the Criteria for Baseline Cybersecurity Control Frameworks is in Appendix 1 (CIS CSC 20) and Appendix 2 (FSC Profile) of this report.

Figure 2 (Revisited) – The tiered approach to cybersecurity controls



7. Center for Internet Security Top 20 Critical Security Controls

Figure 3 – Common, minimum standards and controls across all market activities



7.1 CIS CSC 20: overview

The CIS CSC 20 controls, currently in version 7.1, can be applied in any jurisdiction. They are presented in priority order, use relatively simple language and offer themselves as a layered set of building blocks within a security roadmap for FinTechs.

This CIS CSC 20 recognizes that increasing the complexity of controls doesn't necessarily provide better security. Organizations should initially focus on a smaller set of practices that provide both high security value as well as a foundation for a more advanced and tailored defence.

7.2 CIS CSC 20: benefits to FinTechs

Simplicity

The simplicity of the CIS CSC 20 recommendations is in their favour. Using the CIS CSC 20, the control environment needs to become more sophisticated only as the organization's business and technical environment becomes more complex, as a firm's understanding of its risk environment warrants more defensive effort or as an increase in its size or the range of services offered requires it to comply with an increasing number of standards.

Prioritization

The CIS CSC 20 provides a prioritized list of controls based on a regularly updated set of common cybersecurity risks. This model provides clear efficiencies for firms with limited resources.

Ease of implementation

The suite of self-assessment and implementation tools built around the CIS CSC 20 is continuously improved and has shown itself adaptable to commercial activities such as mergers and acquisition (see case study in Appendix 2). This makes it an attractive starting point for low-maturity FinTechs looking for a clear pathway to enhanced cybersecurity.

7.3 CIS CSC 20: limitations for FinTechs

Controls do not map to financial services cybersecurity regulations

CIS controls do not immediately allow FinTechs to comply with financial services regulations and are not sufficient for many types of partnership with regulated financial services firms, nor are they sufficient for offering financial services to customers.

7.4 CIS CSC 20: conclusion

The CIS top 20 Critical Security Controls provide effective foundational security and a clear roadmap for FinTechs wishing to build a robust cybersecurity programme. If the CIS CSC 20 controls were widely implemented, the level of resilience across the financial system would be greatly improved.

However, the CIS CSC 20 are not designed to map specifically to financial services providers or the regulations to which financial services providers are subject. Tools to make the CIS CSC

20 more readily applicable to financial services are under development. In the meantime, the CIS CSC 20 do not directly support compliance with financial service regulations so are not generally sufficient for partnerships with established financial services firms.

An examination of how the CIS CSC 20 controls compare against the Criteria for Choosing Base-Level Frameworks is in Appendix 2 to this report.



8. The Financial Services Cybersecurity Profile

8.1 Financial Services Cybersecurity Profile: Overview

The [Financial Services Cybersecurity Profile](#) (the FSC Profile) aggregates cybersecurity regulatory requirements from several regions, identifies where requirements are shared and creates diagnostic statements that describe the desired end state that a firm needs to reach in order to be compliant.

These diagnostic statements are then mapped to cybersecurity frameworks such as the National Institute of Standards and Technology (NIST)¹⁹ and International Organization for Standardization (ISO) 27000 so that organizations have a reference point for the implementation of controls.

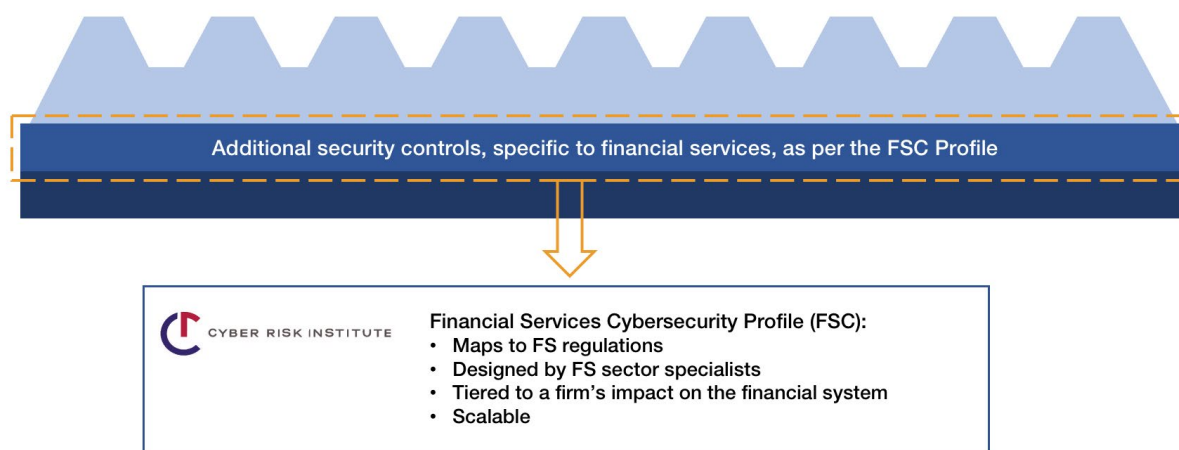


The underlying structure of the FSC Profile ties back to the five core categories of NIST (identify, protect, detect, respond and recover) as well as two additional categories (governance and supply chain management) derived from CPML-IOSCO's 2016 Guidance on Cyber Resilience for

Financial Market Infrastructures²⁰ and financial service regulatory issuances.

From May 2020 the FSC Profile will be maintained by an industry-funded non-profit, the Cyber Risk Institute.²¹

Figure 4 – Tiered approach 2: common, minimum standards and controls mapped to FS regulatory requirements



8.2 FSC Profile: benefits to FinTechs

The FSC Profile facilitates regulatory compliance

The FSC Profile streamlines the process of complying with varying regulatory regimes and is adapted for markets in North America, Europe and Asia-Pacific. This efficiency enables growing FinTechs, which are often subject to multiple regulatory regimes even in their early stages, to move their focus from compliance activity to protecting their clients and assets.

It synthesizes more than 2,300 cyber regulatory provisions into a set of 277 diagnostic statements mapped back to those provisions, which are then further narrowed by the implementing firm's impact on the economy should it be felled by a cyber incident. In the lowest-impact tier, at which many smaller FinTechs would sit, the number of diagnostic statements has been narrowed to 145.²²

The FSC Profile facilitates commercial partnerships

Because the FSC Profile maps to financial services regulations and has the support of major US and European financial services firms,²³ it will facilitate many types of partnership between FinTechs and regulated financial services firms operating in these regions. It has the potential to be scaled globally as it integrates regulations from more regions through its regular update process.

Several of these organizations have reiterated a commitment to applying the profile through their membership of the Cyber Risk Institute and have committed to applying the profile internally and in their dealings with third parties.²⁴ This guaranteed minimum level of industry support expands the profile's potential to provide a return on investment to FinTechs in the form of a mutually understood approach to cybersecurity controls.

Enhanced guidance and tools to support implementation

The Cyber Risk Institute has outlined a three-year plan to enhance its maturity model, develop controls implementation and self-assessment tools, accelerate adoption of the profile's use across the private sector and to support

supervisory bodies that wish to examine a regulated firm's cybersecurity using the profile.

With the addition of further guidance and implementation tools, the profile has the potential to become a roadmap for FinTechs wishing to expand and do business with established financial services providers.

8.3 FSC Profile: limitations for FinTechs

Relative complexity of the profile

The integration of regulatory requirements²⁵ into the FSC Profile is desirable but creates a larger set of minimum requirements than would exist absent regulatory considerations. CIS CSC 20, for example, is not tied to regulatory requirements and thus presents a smaller, more digestible menu of controls to implement.

The FSC Profile aims at cyber resilience through regulatory compliance. This adds a layer of complexity to the diagnostic statements as they must be mapped to regulations and then cross-referenced to cybersecurity sources, such as the NIST CSF and ISO 27000 series. For a low-maturity company, this can obscure the purpose of the diagnostic statement and make it difficult to understand how to implement the required controls. We acknowledge the Cyber Risk Institute's plans to develop guidance for implementation and evidencing compliance with the profile's diagnostic statements.

Volume of controls

The FSC Profile greatly reduces the number of regulatory requirements that a FinTech might need to review. Nonetheless, there are many in-scope controls – they can range in number from 136 to 277 depending on the potential geographical impact of the firm (from localized to super-national).²⁶

Difficult to prioritize and implement diagnostic statements

Many controls are people and process-oriented, with the FSC Profile being light in terms of technical controls that are the most problematic for FinTechs to prioritize and implement.

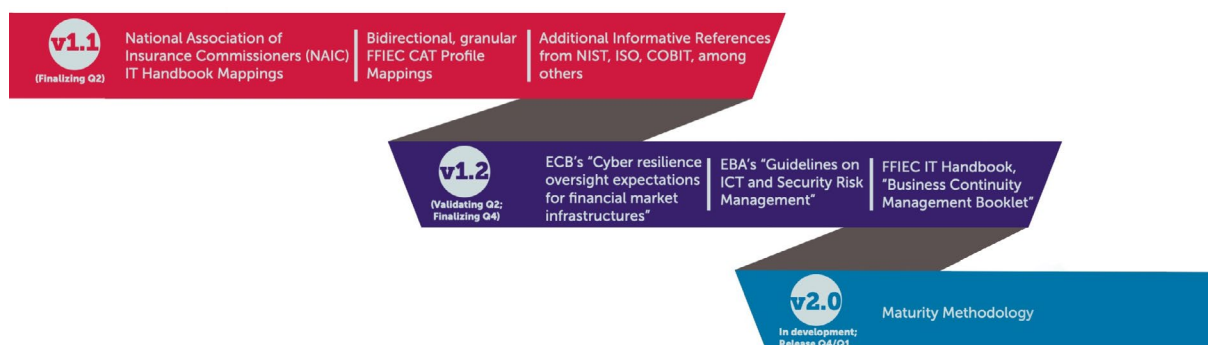
The FSC Profile's control statements as presented imply equal importance for each control. There is no prioritization, sequencing or implementation group that would lend itself to building and executing a security improvement roadmap in a small FinTech. At the time of publication, the Cyber Risk Institute was developing an enhanced maturity rating and weighting system to remedy this.

Support tools are not yet ready

Self-assessment tools are currently under development. In its current v1.0 form, the FSC Profile scoring for a control statement is limited to yes, no or N/A.

Examples of evidence that could be provided to help demonstrate that a control is in place and operating effectively are not yet available to use. However, these are under development.

8.4 The Financial Services Cybersecurity Profile: conclusion



With the launch of the Cyber Risk Institute in May 2020, the FSC Profile is at an inflection point in its development. As further guidance and implementation tools are added – as the Cyber Risk Institute indicates will occur – the profile will grow in relevance and applicability to FinTechs.

The FSC Profile streamlines the process of complying with multiple and varying regulatory regimes. This efficiency enables FinTechs to focus their efforts on protecting their clients and assets rather than on compliance activity.

The FSC Profile is structured to assist financial institutions in assessing their cybersecurity risk-management governance, processes, capabilities, and regulatory compliance posture. It goes beyond the technical cybersecurity controls seen in the CIS CSC 20.

These extra layers, many of which are specific to regulated entities in financial services, mean that the FSC Profile adds value for its users and potentially for financial supervisors and examiners. Inevitably, these layers also add complexity, and low-maturity FinTechs may find it more effective to begin their foundational work by using the CIS CSC 20.

The new custodian of the profile, the Cyber Risk Institute, has funded plans that could reduce the challenges faced by low-maturity FinTechs and other small financial institutions. Nonetheless, based on the currently available version of the profile, the CIS CSC 20 is preferred for foundational work on cybersecurity controls. Once this is defined and underway, then the profile can be used to help take the security programme to the next level.

9. Conclusion

The Consortium believes that the security of the wider financial system requires the acceleration of FinTechs’ access to methodologies for identifying cybersecurity risks and applying the practical steps needed to mitigate them. These methodologies should be scalable, meaning they can be applied across borders so that a FinTech can use recognized cybersecurity best practice to facilitate entry to new markets and grow securely as it expands.

To support the effective implementation of controls, a holistic security management system should be developed that accounts for the interplay between controls, assessment, metrics and regulation. This would enable growing companies to map security controls to the assets and processes that provide value to their business, as well as their partners and customers. In turn, this will support them in prioritizing their resources as they define, build out and adapt their security programmes.²⁷

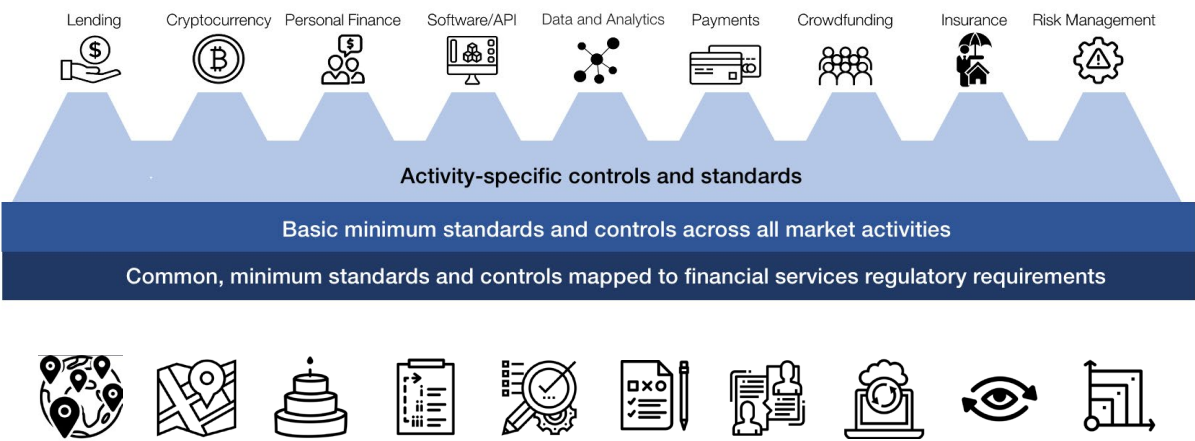
The starting point for this is an effective risk-based controls framework and assessment procedure that includes common guidance on the choice and implementation of a recognized set of cybersecurity controls for FinTechs.

The solution should start with baseline requirements for controls and assessment but provide an increasing complexity of controls as organizations develop and their cybersecurity risk-management requirements mature.

Cybersecurity controls require regular adaptation as technology, threats and business models change. Controls are granular, specific to the assets they are meant to protect, and may have a limited shelf life. Consequently, we recommend that cybersecurity controls should be defined by financial services providers, where the expertise and funding can be deployed at speed, in consultation with cybersecurity experts from other sectors, governmental agencies and relevant civil-society organizations.

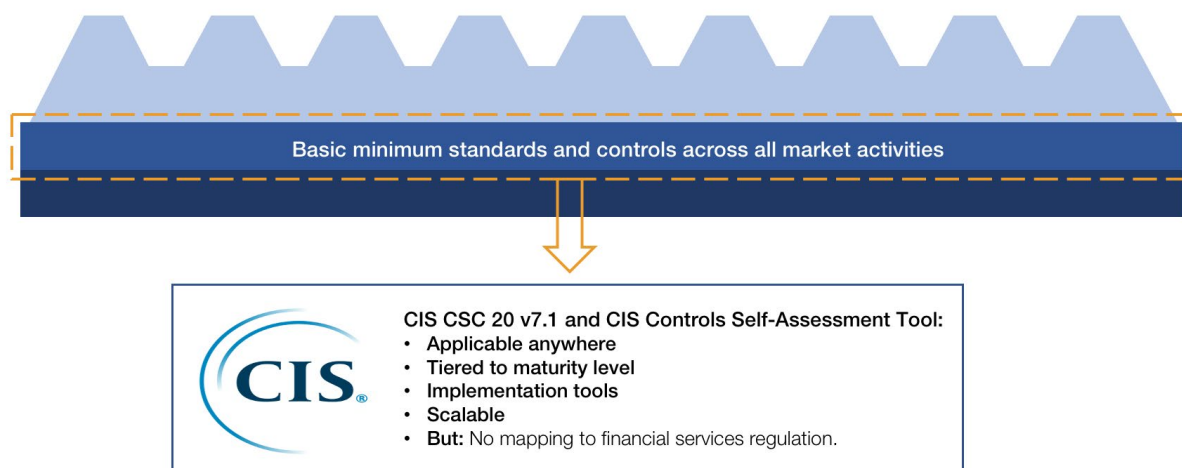
The findings of the World Economic Forum’s FinTech Cybersecurity Consortium provide a starting point and set a challenge to continue building towards a security management system that enables FinTechs to be the engine of innovation the industry is looking for.

Figure 5 – The tiered approach to cybersecurity controls with consideration criteria



10. Appendix 1: The CIS CSC 20 vs. base-level controls criteria

Figure 3 (Revisited) – Common, minimum standards and controls across all market activities



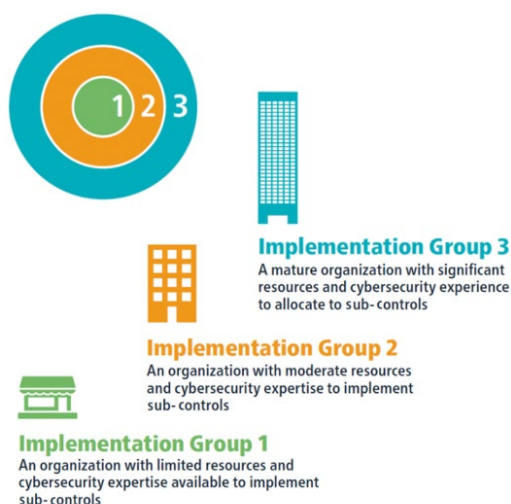
Applicable anywhere

The CIS CSC 20 can be applied to any business sector in any jurisdiction.

Controls map to accepted standards and regulation

The CIS CSC 20 do not map to financial services regulation. They are designed to support technical security and not regulatory compliance.

Tiering



The CIS CSC 20 is tiered to maturity levels, called implementation groups, based on an organization's size, resources and the sensitivity of data an organization is responsible for protecting. This provides a roadmap for growth that supports the development of cybersecurity controls implementation time.

Prioritization

CIS CSC 20 offers a prioritized set of actions to protect organizations and the data of organizations from known cyberattacks.

Self-assessment

The CIS Controls Self-Assessment Tool (CSAT) is a free web-based tool that helps organizations assess their current implementation of the CIS CSC 20 and track how their implementation changes over time.

Results can be exported in different formats, including slides, to facilitate discussions with business leadership and non-technical teams.

CIS CSAT: beyond self-assessment

A US-based member of the Forum's FinTech Cybersecurity Working Group adapted the CIS Critical Security Controls (CSC) framework for use, but also as a key element of a merger and acquisition project.

During due diligence of an Asia-Pacific acquisition target, the CIS CSC was used as a basis for security due diligence questions that were general enough to be portable across regions and service offerings, but specific enough to provide real insight into the maturity of the target's security controls.

After the acquisition was closed, the CIS Controls Self-Assessment Tool (CSAT) was used to perform a gap analysis and to build a joint remediation plan. The structure of the CSC framework enabled the firms to build a practical and achievable plan since the controls are prioritized, assessed against a maturity model and described in clear, understandable terms. Since the CIS CSC was used by both parties as a source of baseline security controls, it formed a common language that helped accelerate the integration of their security programmes.

Implementation tools: measuring the effectiveness of controls implementation

The CIS CSC 20 Controls Assessment Specification as applied to financial services

The CIS maintains a Controls Assessment Specification (CAS) that is sector-agnostic and can be built upon to provide sector-specific metrics for the financial services sector.

The CAS aims to provide a common understanding of what to measure in order to verify that CIS sub-controls are properly implemented. In order to support as many different types of organizations and sectors as possible, it does not comment on "how to measure".

To optimize the measurement of the CSCs, it must be as automated as possible. At the time of publication, CIS is engaging with software security vendors and governance, risk and compliance vendors to implement CAS within their tooling before the end of 2020. This is a positive development that could greatly enhance the utility of the CIS CSC 20 framework to FinTechs.

Peer-to-peer comparison

The CIS CSC CSAT tool can be used to create industry averages as a point of comparison against peers in each sector.

Aggregate scores from users provide data that CIS can use to help improve future versions of the CIS Controls as well as furnishing information security and compliance teams with a clear industry comparison that they can provide to their executive board. This helps boards clarify where and why they need to release resources to information security teams.

Table 1 – Highest-scoring sub-controls

Rank	Sub-control title	Average cross-sector score	Implementation group (maturity tier)
1	Ensure anti-malware software and signatures are updated	81.42	1
2	Use centrally managed anti-malware software	80.00	2
3	Employ the Advanced Encryption Standard (AES) to encrypt wireless data	79.69	1
4	Create separate Wi-Fi network for untrusted devices	78.53	1
5	Maintain an inventory of authorized wireless access points	76.75	2

Table 2 – Lowest-scoring sub-controls

Rank	Sub-control title	Average cross-sector score	Implementation group (maturity tier)
171	Create a test bed for elements not typically tested in production	12.50	2
170	Use an active discovery tool to identify sensitive data	13.78	3
169	Use dedicated workstations for all administrative tasks	14.92	3
168	Enforce access control to data through automated tools	15.05	3
167	Perform periodic red team exercises	15.33	3

Regular update cycles

The CIS CSC 20 controls are maintained by the US-based non-profit Center for Internet Security.²⁸ They are regularly updated and are currently on version 7.1.

The CSAT tool is subject to ongoing improvements to support ease of use.²⁹

Potential for external validation

Many organizations use the CIS Critical Security Controls (CSCs) to prove to auditors that they meet requirements in multiple regulatory frameworks as well as to improve cybersecurity within their enterprise.

Scaling

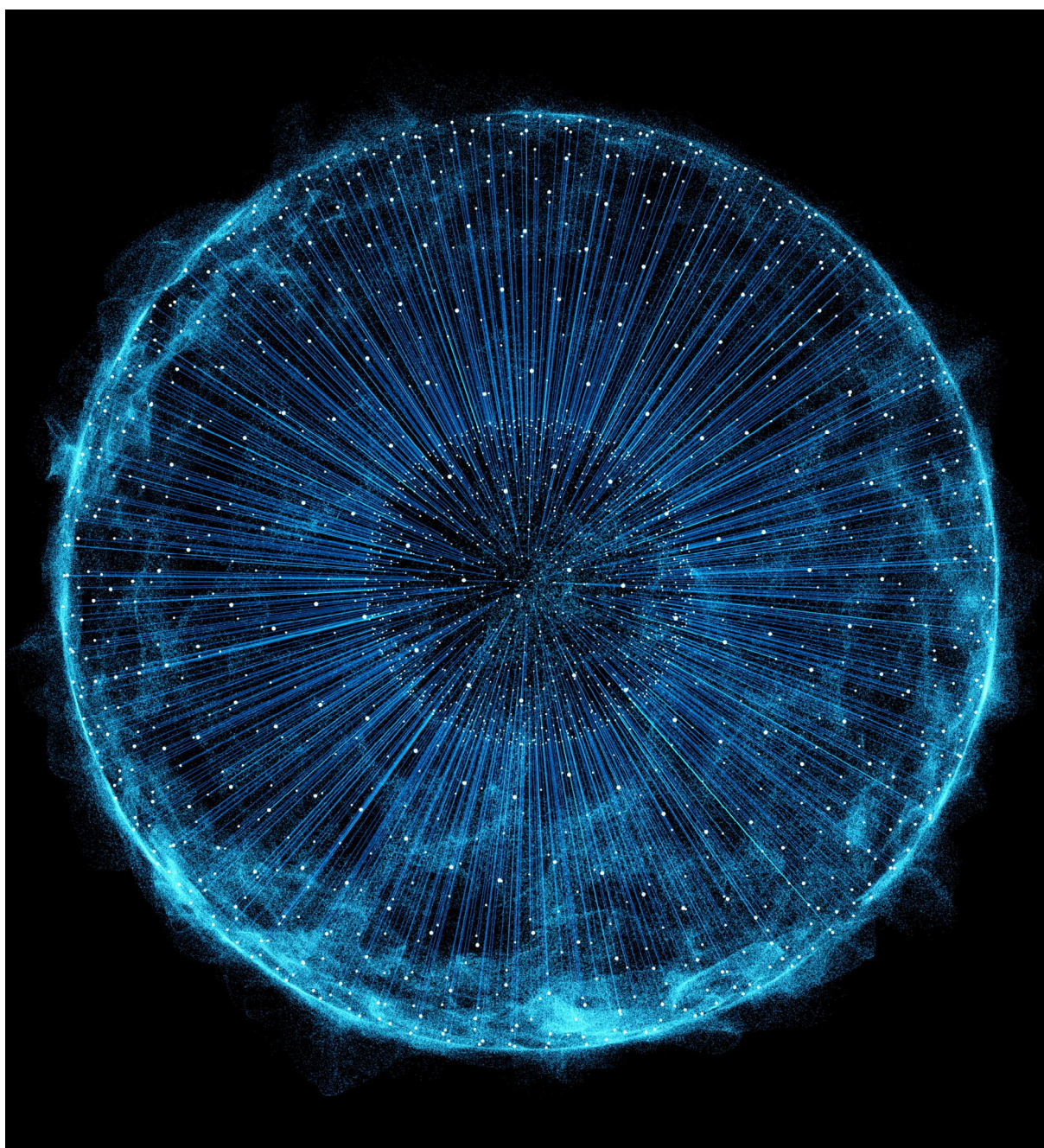
The CIS CSC 20 controls framework has the potential for scaling, including indications of support from major financial services regulators, central banks or international organizations with responsibility for safeguarding the resilience of the financial system.

In August 2019, the United States Federal Financial Institutions Examination Council (FFIEC) made a call to standardize approaches to assessing cybersecurity preparedness.³⁰ The FFIEC's call referenced CIS CSC 20 alongside the FFIEC's own cybersecurity assessment tool,

the FSSCC Cybersecurity Profile (discussed later in this report) and the NIST Cybersecurity Framework.

The CIS CSC 20 has also been mentioned as a prominent standard by CPMI-IOSCO and the Alliance for Financial Inclusion.³¹

While the CIS CSC 20 is not generally sufficient to comply with financial services regulatory requirements, it remains a stepping stone towards compliance and an applicable baseline from which to build cybersecurity controls implementation tools and implementation guidance for FinTechs.



11. Appendix 2: The FSC Profile vs. base-level controls criteria

11.1 The future of the Financial Services Cybersecurity Profile



The FSC Profile was developed via a financial services industry body, the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security ([FSSCC](#)) in the United States. It was released in October 2018.

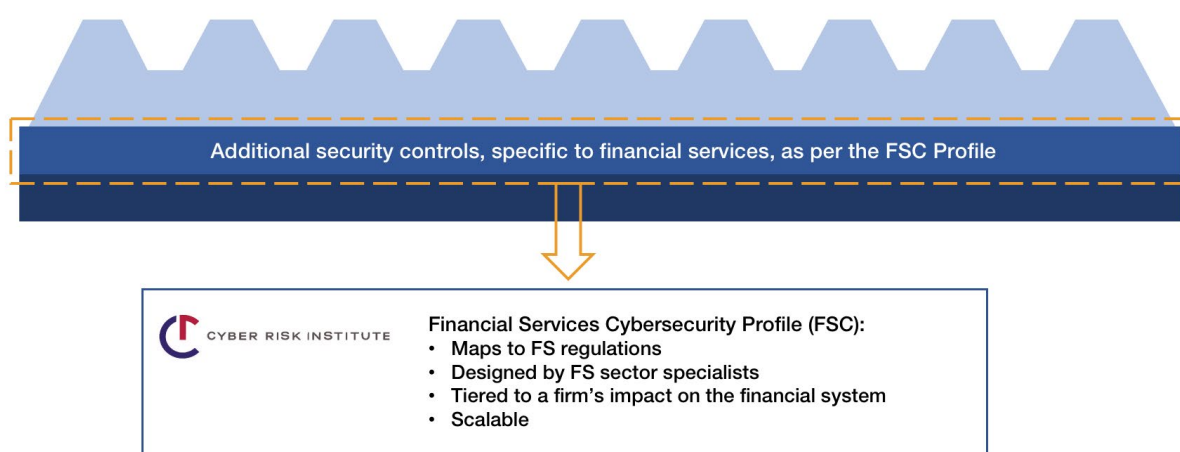
From 2020, intellectual property rights over the FSC Profile sit with a financial services sector-funded non-profit, the Cyber Risk Institute.³²



The growth strategy for the FSC Profile: build, use, educate and integrate

The Cyber Risk Institute has committed to keeping a free-to-access spreadsheet version of the FSC Profile, to integrating additional regulatory regimes from across the globe and developing guidance for firms and regulators to assist in its use and acceptance. It also has plans to offer an enhanced FSC Profile user interface to its members and continues to meet with interested financial supervisors to explain the FSC Profile's benefits to the regulators and provide training for its use. Cyber Risk Institute members have committed to using the profile for their own self and regulatory assessment purposes and in their own business activities and partnerships.

Figure 4 (Revisited) – **Tiered approach 2: common, minimum standards and controls mapped to FS regulatory requirements**



11.2 The FSC Profile vs. base-level controls criteria

Applicable anywhere

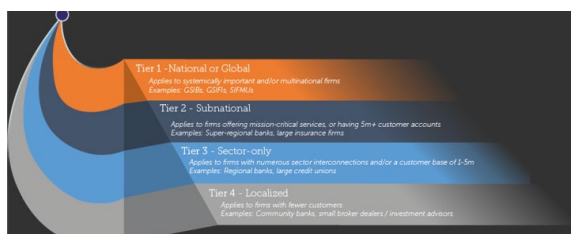
The FSC Profile v1.0 maps to most regulations in North America and a smaller proportion of regulations in Europe and Asia-Pacific. Beginning in 2020, the Cyber Risk Institute plans to incorporate three to five pieces of international (non-US) regulation per year. This will expand the geographical application of the FSC Profile.

Controls map to accepted standards and regulation

The FSC Profile synthesizes more than 2,300 regulatory provisions into 277 diagnostic statements. These statements are mapped to financial services regulations and then cross-referenced to notable cybersecurity frameworks such as the NIST Cybersecurity Framework, the ISO 27000 series, the CIS CSC 20 and others.

Tiering

The profile is tiered based on the impact a firm would have on the financial system if it were felled by a cyber incident. The four tiers – tier 1: national/super-national impact; tier 2: sub-national impact; tier 3: sector impact; and tier 4: localized impact – are determined through a nine-question questionnaire that bases its determinations on existing governmental designations (e.g. Global Systemically Important Bank [G-SIB] and Global Systemically Important Financial Institution [G-SIFI]), geopolitical risk, consumer impact and interconnectedness.



Self-assessment

The Cyber Risk Institute has committed to developing a diagnostic-statement-by-diagnostic-statement guide with examples of effective evidence that institutions can use to support self-assessment and external examination.

Peer-to-peer comparison

Not available in v1.0 of the FSC profile.

Regular update cycles

The profile is updated on a regular basis on the recommendations of the Cyber Risk Institute's members. Full updates to the profile are to be provided every two to three years.

Potential for external validation

The Cyber Risk Institute has committed to educating financial services supervisors and cybersecurity examiners in government agencies in assessing against the profile. This creates a high potential for effective external validation.

Scaling

The FSC Profile controls framework has the potential for scaling, including indications of support from major financial services regulators, central banks or international organizations with responsibility for safeguarding the resilience of the financial system.

In August 2019, the United States Federal Financial Institutions Examination Council (FFIEC) made a call to standardize approaches to assessing cybersecurity preparedness.³³ The FFIEC's call referenced CIS CSC 20 alongside the FFIEC's own cybersecurity assessment tool, the FSSCC Cybersecurity Profile and the NIST Cybersecurity Framework.

The FSC Profile has also been mentioned as a prominent standard by CPMI-IOSCO and the Alliance for Financial Inclusion.³⁴

12. Appendix 3: The role of industry and public-private initiatives

This report concentrates on FinTechs because of their increasing importance to the security of the financial system. As technological and policy changes lead financial services to become more modularized, with client data and assets spread across multiple providers, we expect the importance of FinTechs creating a cyber-resilient financial system to increase.

However, enhancing cyber resilience across financial services is about more than controls and assessment. It requires the education and protection of smaller service providers. Industry groupings and public-private coalitions have an important role to play in educating and supporting smaller traditional organizations such as credit unions, building societies and merchants.

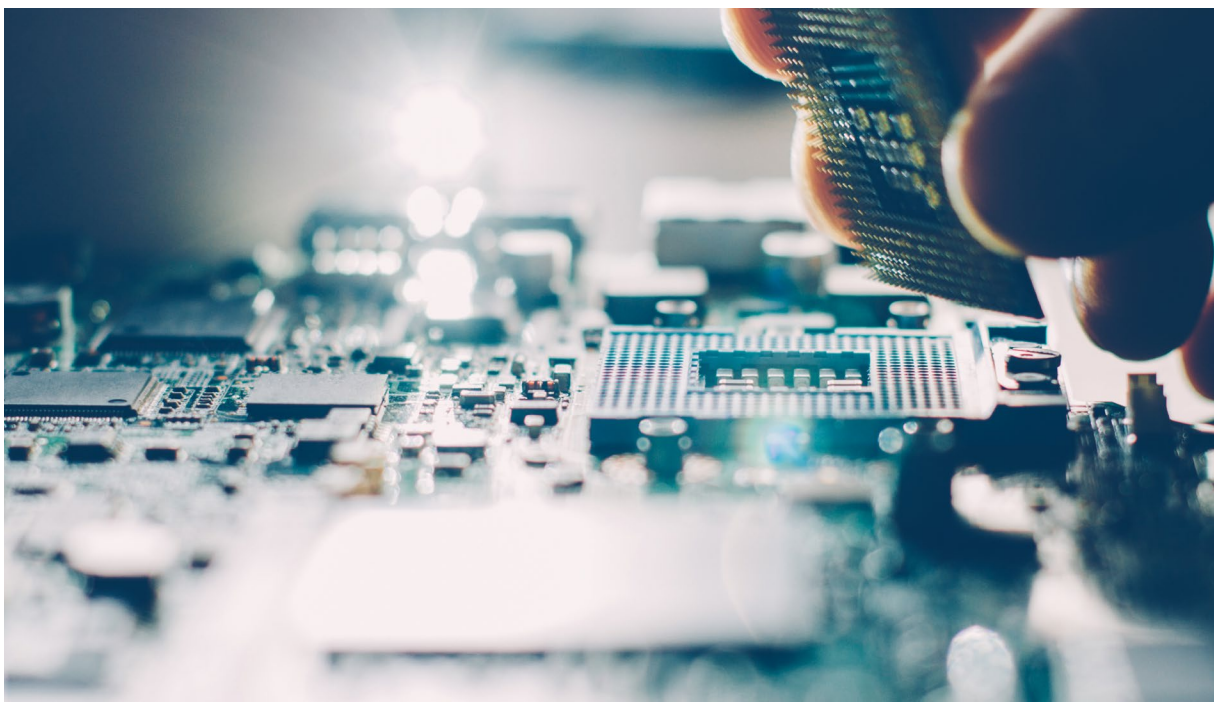
General-purpose toolkits provide accessible guidance on cybersecurity that goes beyond the specifics of controls frameworks. The *Capacity-Building Tool Box for Financial Organizations*³⁵ developed via the Carnegie Endowment for International Peace, with support from the SWIFT Institute, the Financial Services Information Sharing and Analysis Center (FS-ISAC),

the Cyber Readiness Institute, the Global Cyber Alliance, the International Monetary Fund and Standard Chartered Bank, distils depth and breadth of expertise into short, achievable one-page guides for low-maturity businesses.

Guidance specific to particular areas of financial services is often developed by industry associations, such as the Payments Card Industry (PCI) Security Council series on Data Security Essentials for Small Merchants, which includes the Guide to Safe Payments,³⁶ and provides accessible and achievable guidance that protects merchants and customers without requiring a sophisticated information security department.

Individual corporate initiatives such as the Mastercard Accelerate³⁷ and Start Path³⁸ programmes provide support for start-ups and emerging brands at every stage of their growth and transformation.

Cybersecurity is collaborative and the recommendations in this report are intended to benefit from and support ongoing initiatives elsewhere in the financial services sector.



Contributors

Lead Authors

Seán Doyle Project Lead, Platform for Shaping the Future of Cybersecurity and Digital Trust, World Economic Forum (Switzerland)

Working Group members

Adrienne Allen Director of Security GRC and Privacy, Coinbase (USA)
Parker Crockford VP of Growth at UPvest (Germany)
Jonathan Davis Senior Director, Cybersecurity Policy and Awareness, Visa (UK)
Sabina Frizell Manager, Global Public Policy, Visa (USA)
Jason Harrell Head of Business and Government Cybersecurity Partnerships, DTCC (USA)
Jim Maloney Chief Security and Privacy Officer, Social Finance (SoFi) (USA), World Economic Forum Expert Network Member
Michael Nunes Senior Director and Head of Government Advisory, Visa (USA)
Bruce Rutherford Senior Vice-President, Security Standards & Solutions, Mastercard (USA), Chairperson of the Executive Committee of the Payment Cards Industry Security Standards Council
Adam Sommer Vice-President, Industry Standards, Mastercard (USA)
Sam Taussig Head of Global Policy, Kabbage (USA)

World Economic Forum

Mary-Emma Barton Research and Analysis Specialist, Platform for Shaping the Future of Financial and Monetary Systems
Matthew Blake Head, Platform for Shaping the Future of Financial and Monetary Systems
Georges De Moura Head of Industry Solutions, Platform for Shaping the Future of Cybersecurity and Digital Trust
Daniel Dobrygowski Head of Corporate Governance and Digital Trust, Platform for Shaping the Future of Cybersecurity and Digital Trust
Kai Keller Project Lead, Platform for Shaping the Future of Financial and Monetary Systems
Marie Sophie Mueller Programme & Engagement Lead, Platform for Shaping the Future of Cybersecurity and Digital Trust

With thanks to:

Ghiyazuddin Mohammad, Alliance for Financial Inclusion (Malaysia); Jacques Francoeur, ITU-T Study Group 17: Security; The Monetary Authority of Singapore; Troy Leach, CTO Payment Card Industry Security Standards Council; Curtis Dukes and Phyllis Lee, Center for Internet Security; Josh Magri and Alan Carroll, Cyber Risk Institute

Endnotes

1. World Economic Forum, The Global Risks Report 2020:, http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf (link as 26/5/20).
2. Most notably, the NIST Cybersecurity Framework: <https://www.nist.gov/cyberframework>, and ISO/IEC 27002: <https://www.iso.org/standard/54533.html> (links as of 26/5/20).
3. For example, The EU Network and Information Security Directive (NIS): <https://www.enisa.europa.eu/topics/nis-directive>, and the EU's General Data Protection Regulation (GDPR): <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504> (links as of 26/5/20).
4. For example, the Center for Internet Security Critical Security Controls: <https://www.cisecurity.org/>, and the HITRUST Cybersecurity Framework: <https://hitrustalliance.net/hitrust-csf/> (links as of 26/5/20).
5. For an example, see the well-received Cyber Resilience and Financial Organizations: A Capacity-Building Tool Box, 2019, from Carnegie Endowment for International Peace: <https://carnegieendowment.org/specialprojects/fincyber/guides>. A less explicit but equally valuable approach to capacity building can be found in the PCI Security Council's series on Data Security Essentials for Small Merchants: https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf (links as of 26/5/20).
6. For example, GSMA Mobile Money Certification for the mobile payments sector: <https://www.gsma.com/mobilefordevelopment/mobile-money/certification/>. In the public sector, the US FedRAMP is also notable: <https://www.fedramp.gov/> (links as of 26/5/20).
7. See, for example, the work of the Vendor Security Alliance: <https://www.vendorsecurityalliance.org/> (link as of 26/5/20).
8. Alliance for Financial Inclusion, Cybersecurity for Financial Inclusion: Framework and Risk Guide, October 2019: <https://www.afi-global.org/publications/3146/Cybersecurity-for-financial-inclusion-framework-risk-guide> (link as of 26/5/20).
9. The spread of the TIBER-EU approach to ethical red teaming – itself growing from the Bank of England's CBEST framework – shows how regulators can provide a governance framework for systemically important banks that shines a light on risks across the wider financial sector.
10. Conclusions based on meetings of central banks and governmental authorities from the financial services and aviation sectors at the World Economic Forum's Annual Meeting on Cybersecurity, November 2019.
11. FinTech Cybersecurity Consortium workshops were held in New York in October 2018 and July 2019, Singapore in November 2018 and London in November 2018 and March 2019. This was tested with a wider audience at the Forum's Annual Meeting on Cybersecurity in November 2019. Our thanks also go to the Alliance for Financial Inclusion for insight gained at meetings of financial services supervisors in Prague, Czech Republic, in September 2019 and Kuala Lumpur, Malaysia, in February 2020.
12. PCI Security Standards Council, PCI Security: https://www.pcisecuritystandards.org/pci_security/ (link as of 26/5/20).
13. World Economic Forum, Innovation-Driven Cyber-Risk to Customer Data in Financial Services, 2017: http://www3.weforum.org/docs/WEF_Cyber_Risk_to_Customer_Data.pdf (link as of 26/5/20).

14. Various held in New York in October 2018 and July 2019, Singapore in November 2018 and London in November 2018 and March 2019.
15. Such as through security and penetration testing.
16. Findings from the World Economic Forum Annual Meeting on Cybersecurity 2019. Sessions on Supply-Chain Security and Cybersecurity in the Financial System, November 2019.
17. Ibid.
18. Cyber Risk Institute, FSC Profile: <https://cyberriskinstitute.org/> (link as of 28/5/20).
19. The profile's development benefited from being featured at open workshops run at NIST risk-management conferences in the US and maps well to the NIST cybersecurity standard. NIST Cybersecurity Workshop, Financial Services Sector Specific Cybersecurity Profile, 18 May 2017: https://www.nist.gov/system/files/documents/2017/05/18/financial_services_csf.pdf (link as of 26/5/20).
20. Committee on Payments and Market Infrastructures, Guidance on Cyber Resilience for Financial Market Infrastructures, Bank for International Settlements and International Organization of Securities Commissions, 2016: <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf> (link as of 26/5/20).
21. Disclosure: A member of the World Economic Forum's Platform for Cybersecurity and Digital Trust sits on the [managing board of the Cyber Risk Institute](#) for the period 2020–2022. The Forum's participation in the Cyber Risk Institute began in 2020, after the period in which work on this report was undertaken and its recommendations developed.
22. Financial Services Sector Coordinating Council (FSSCC), Financial Services Sector Cybersecurity Profile: <https://fsscc.org/Financial-Sector-Cybersecurity-Profile> (link as of 26/5/20).
23. The profile was developed using a consensus-based process similar to that of other standards-setting bodies (e.g. ISO and NIST). More than 150 financial institutions, including large multinationals, market utilities, insurers, asset managers, payment companies and community institutions provided their input and expertise.
24. Cyber Risk Institute, Less Risk. More Rewards: <https://cyberriskinstitute.org/impact/> (link as of 29/5/20).
25. This includes NIST, ISO/IEC 27001; the CIS CSC 20; COBIT.
26. FSSCC, Financial Services Sector Cybersecurity Profile: <https://fsscc.org/Financial-Sector-Cybersecurity-Profile> (link as of 26/5/20).
27. A "unified security model" has been proposed in the 2020 update to the International Telecommunication Union (ITU) Security Manual, which would map "value-creating assets" in a business to the cybersecurity controls that protect them: https://www.itu.int/wftp3/Public/epub_shared/TSB/2015-Security-Manual/mobile/index.html#p=1 (link as of 27/5/20).
28. Center for Internet Security (CSI): <https://www.cisecurity.org/> (link as of 26/5/20).
29. Updates are flagged through the CSAT user community page: <https://workbench.cisecurity.org/communities/91> (link as of 27/5/20).
30. FFIEC, FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness, 28 August 2019: <https://www.ffiec.gov/press/pr082819.htm> (link as of 26/5/20).

31. International Organization of Securities Commissions, Cyber Task Force Final Report, June 2019: <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD633.pdf>; Alliance for Financial Inclusion, Cybersecurity for Financial Inclusion: Framework & Risk Guide, October 2019: <https://www.afi-global.org/publications/3146/Cybersecurity-for-financial-inclusion-framework-risk-guide> (links as of 28/5/20).
32. Disclosure: A member of the World Economic Forum's Platform for Cybersecurity and Digital Trust sits on the [managing board of the Cyber Risk Institute](#) for the period 2020–2022. The Forum's participation in the Cyber Risk Institute began in 2020, after the period in which work on this report was undertaken and its recommendations developed
33. FFIEC, FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness, 28 August 2019: <https://www.ffiec.gov/press/pr082819.htm> (link as of 26/5/20).
34. International Organization of Securities Commissions, Cyber Task Force Final Report, June 2019: <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD633.pdf>; Alliance for Financial Inclusion, Cybersecurity for Financial Inclusion: Framework & Risk Guide, October 2019: <https://www.afi-global.org/publications/3146/Cybersecurity-for-financial-inclusion-framework-risk-guide> (links as of 28/5/20).
35. Carnegie Endowment for International Peace, Cyber Resilience and Financial Organizations: A Capacity-Building Tool Box: <https://carnegieendowment.org/specialprojects/fincyber/guides> (link as of 26/5/20).
36. PCI Security Standards Council, Guide to Safe Payments, August 2018: https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf (link as of 26/5/20).
37. Mastercard Accelerate, <https://www.mastercard.us/en-us/business/issuers/grow-your-business/fintech.html> (link as of 22 June 2020)
38. Mastercard Start Path, <https://startpath.mastercard.com/spglobal/home.html> (accessed 22 June 2020)



COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744

contact@weforum.org
www.weforum.org