Practices and Tools required to support Risk-based Supervision in the Digital Age

November 2018

Acknowledgements

The International Financial Consumer Protection Organisation (FinCoNet) would like to acknowledge the efforts of Standing Committee 4 (SC4) in developing and finalising this project. Standing Committee 4 consists of representatives from Australia, Brazil, Canada, Germany, Indonesia, Japan, Mauritius, Portugal, Russia, South Africa and Spain and had the assistance of staff from the OECD Secretariat. In particular, we would like to thank Roberto España as Chair of the Committee as well as Luís Neto Raposo, Ana Raquel Ruivo, Sina Weinhold-Koch, Barbara Pohl, Michael Blyth, Vidhi Mahajan, Tara Marshall, Takaaki Hattori, Kosuke Ito, Hiroko Suzuki, Ramsamy Chinniah, Urvashi Soobarah, Gouro Sall Diagne, Francisco José Barbosa da Silveira, Maria Emília Moretti, Caroline da Silva, Hudiyanto, Sudha Hurrymun, Teresa Frick, Elena Nenakhova, Monica Griga, Elena Barrado and Isabel Torre, for their work in writing and producing the survey and report.

FinCoNet would also like to express its full appreciation to all respondents to its survey, *Practices and Tools Required to Support Risk-Based Supervision in a Digital Age*.

About FinCoNet

FinCoNet was established in 2003 as an informal network of financial consumer protection regulators and supervisors to discuss and share experiences on consumer protection issues of common interest. It is recognised by the Financial Stability Board (FSB) and Group of 20 (G20).

In November 2013, FinCoNet was formalised as a new international organisation of financial consumer protection supervisory authorities.

The goal of FinCoNet is to promote sound market conduct and enhance financial consumer protection through efficient and effective financial market conduct supervision, with a focus on banking and credit.

Members see FinCoNet as a valuable forum for sharing information on supervisory tools and best practices for consumer protection regulators in financial services.

Disclaimer

This publication is based on responses to a survey that were received between July and December 2017. Eventually, some respondent jurisdictions have updated the references.

CONTENTS

Graphs

Tables

EXECUTIVE SUMMARY

Technology is rapidly transforming the world, particularly the financial services sector. This transformation has the potential to increase competitiveness, innovation and efficiency, creating real benefits for both consumers and financial entities. However, the provision of digital financial products and services also creates risks for consumers.

Digital financial products and services (DFPS) are understood in this report to be financial products and services commercialised by bank or non-bank institutions through digital channels (online or mobile). This definition comprises two different dimensions: the channels through which products and services are made available to clients who access them via online internet browsers or mobile apps on their digital devices; and the products and services that are commercialised through these channels. These products and services may be essentially the same as those marketed through more traditional channels other than (or in addition to) the digital ones (such as depositing, withdrawing, sending and receiving money, payments services, monitoring personal financial information, consumer credit, etc.). Alternatively, they may be products and services that exist only in digital format (such as cryptocurrencies). Accordingly, references in this report to “traditional products” should be understood as traditional products commercialised through traditional channels (such as in-person transactions at a bank branch).

Supervisors now face an enormous challenge in adapting their current supervisory approach to DFPS. They have to find a balance between ensuring financial system soundness and adequate consumer protection on the one hand, while allowing or even fostering technological advances on the other hand. Adequate consumer protection implies respect for the principle of technological neutrality by which consumers should have the same level of protection regardless of the channels and providers used to acquire financial products and services.

In recent years, the most relevant organisations representing financial consumer protection authorities have stressed the need to focus on the effects of digital transformation, mainly from a regulatory perspective. FinCoNet decided to explore the practices and tools required to support risk-based supervision in the digital age, with a market conduct supervisory focus. This work complements that of FinCoNet Standing Committee 1 in compiling a supervisory toolbox that gathers together tools used by FinCoNet members.

For this purpose, FinCoNet developed a survey to collect relevant examples of supervisory practices that are innovative and forward-looking. FinCoNet members and non-members responded to the survey and shared their insights, experiences and practices among the conduct supervision community during the second half of 2017. Due to the high speed of technological change, supervisors have to continuously adapt their tools. For this reason respondents have frequently updated their original input in the course of 2018.

This report analyses supervisory reaction to the digitalisation phenomenon. While there is a broad concern about the nature and size of the challenge, the supervisory approaches towards digital transformation of those who responded to the survey (respondent authorities) are at different stages of development. In most cases, authorities focus predominantly on adapting traditional supervisory tools to DFPS, while the creation of new specific tools is frequently still in the early stages.

Therefore, conclusions must be taken with a note of caution. For this reason, the main findings of this report are not set out under the form of guidance but incorporated as possible learnings under the form of “takeaways” that, from a more informal perspective may give the

supervisory community some idea of the steps followed by peers. Besides, it should be noted that respondent authorities may have perceived the questions differently or be responding from varying positions of knowledge or experience of the subject matter.

In any case, this report includes valuable examples of supervisory tools developed specifically to mitigate risks in a digital environment that are presented as "takeaways" for supervisors. Respondents shared a variety of leading-edge supervisory approaches detailed in the following section highlighting key considerations and takeaways related to DFPS supervision. FinCoNet has identified several topics for supervisors to consider in their design of a supervisory framework for DFPS. Nevertheless, not all the takeaways may necessarily suit all jurisdictions.

The report reviews the diverse regulatory systems among respondent authorities, together with the most common DFPS found across jurisdictions, and the risks they pose. For most authorities, there is an initial phase in addressing DFPS in which traditional supervisory tools are adapted to the digital challenge. Most authorities consider these insufficient and consequently tend to create structures (committees, task forces, etc.) to design new tools for use in supervising DFPS. To fully understand the digital phenomenon, some authorities develop questionnaires to gain industry insight, as long as data reporting on digital aspects is not yet widespread.

To support continuous surveillance of DFPS activity, supervisors need access to standardised data, to adapt complaints handling services that capture information about complaints related to DFPS, to capture relevant information from social media, and to accommodate whistleblowing. On occasion, the licensing process or the approval of new offerings by supervised entities can deepen authorities' understanding of digital developments.

The supervision of DFPS may imply new ways of interacting with supervised entities. Some authorities are developing tools to reproduce, screen-by-screen, the customer's interaction with the digital interface, to check compliance with regulatory requirements.

Authorities responding to the survey acknowledge the challenges in understanding DFPS implications. They frequently recognize the growing need to hire IT experts to support supervision teams, perform specific IT reviews, and analyse the implications of technological outsourcing contracts. The effort to understand better the implications of DFPS is also leading some authorities to consider behavioural economics dimension in their analysis.

The report also analyses the most relevant institutional initiatives followed by some authorities in the field of DFPS: innovation hubs and sandboxes.

We have taken the first steps on a long path that will change the supervisory exercise in the coming years, and supervisors are aware they cannot to lag behind. Therefore, FinCoNet must continuously update its work to address new developments, focusing not only on supervisory tools but also to specific techniques and mechanisms especially designed for digital products and services.

KEY TAKEAWAYS

Table 1 Key considerations and takeaways related to DFPS supervision

Adaptation of traditional tools	Traditional tools may be applicable to DFPS supervision, but some adaptation may be needed, using techniques and procedures incorporating the technological dimension.
Internal steering groups	The creation of internal multidisciplinary working groups (supervision, legal, IT, anti-money-laundering (AML), etc.) can be helpful to gain better understanding of DFPS and determine the supervisory tools to apply to them.
Questionnaires and research	Asking a wide representation of the key players in each jurisdiction to respond to a comprehensive questionnaire may provide insight on the main risks posed by DFPS and determine the possible need for measures to safeguard the interests and rights of consumers.
Close contact with industry, and stakeholders	Regular bilateral meetings and other means of keeping regular contact with supervised entities and other stakeholders can keep authorities informed of DFPS developments and enable their detection of worrisome issues. In addition, valuable input can be obtained from regular meetings with DFPS providers. Other relevant stakeholders may include academics and consumer representatives.
Social media monitoring	Monitoring the mass media and social media may help supervisors to remain up-to-date on new products and emerging risks.
Consumer helpline and whistleblowers	The different schemes to allow whistleblowers to inform supervisors of inappropriate conduct by supervised entities can provide valuable, up-to-date information, particularly in the rapidly changing digital environment.
Complaints handling	Introducing specific codification in the complaints categories to allow the identification of DFPS issues may create a high-potential tool for monitoring and early warning.
Data reporting	Specific data reporting for DFPS is a very important tool that can provide an overview of the digital products and services that are being launched in the market and on their respective characteristics. Security incident reporting should be encouraged to mitigate security risks.
On-site inspections and off-site remote access	To gain insight into the contracting steps customers follow in transactions conducted on the different screens showed on digital devices, supervisors need the right technical tools to access such screens and steps in real time. This is to check whether the screen content and steps respect legal requirements in terms of transparency (pre-contractual and contractual information). These checks could be done with the participation of IT staff employed by authorities. They may review the apps and any other interfaces, including their scripts. IT staff may do so through on-site inspections or off-site remote access to the digital interfaces of the entities in live mode. As technology evolves, new matters become subject to inspection, such as IT systems, big data, scoring models, robot advisors, etc.
Cooperation	There are many reasons for supervisors to engage and cooperate actively and effectively with other authorities in charge of supervision in relation to all DFPS matters. Doing so may help supervisors to gain a broad view of DFPS implications (different sectors, cross-border, technological, anti-money-laundering, data protection, etc.). It may also help to coordinate efforts and avoid overlaps, in order to understand DFPS development and identify potential risks.
Soft regulation	The issuance of supplementary regulatory materials such as guidelines, position notes or warnings may be an effective supervisory tool to discipline certain DFPS segments. These tools may be a valid alternative to amending the global regulatory framework, which may require a long legislative process.

Licensing and authorisation	Regardless of the introduction in the scope of regulation of new entities, the general rules on licensing might be adapted to reflect DFPS risks. This would mean increasing the supervisor's focus on understanding an entity's business model and the nature of new DFPS, and in ensuring the adequacy of the governance arrangements in place with regard to IT systems used to provide DFPS.
Financial education	For most authorities with responsibilities in financial education, there is a clear link between the promotion of the level of financial and digital education of customers, and the impact of efforts to mitigate risks associated with DFPS. Even where financial education is not viewed as a supervisory tool, it may boost the effectiveness of other supervisory tools.
Behavioural economics	DFPS introduce additional complexity to the consumers' decision-making process. The advantages of DFPS to customers–ease and speed of transactions—simultaneously create incentives for consumers to enter into transactions without properly analysing their financial implications. For these reasons, regulators and supervisors should consider behavioural insights as they conduct their activities.
Digital expertise	To face the digital challenge full-on, it may be advisable for supervisors to: • train and keep up to date existing staff so they develop and maintain sufficient technical knowledge to control complex financial technology adequately • increase the number of IT experts available to conduct supervision, and ensure they have specific skills relevant to supervising DFPS • seek that the IT experts working in conduct supervision follow an approach that, building on previous IT risk already developed by many authorities that is often focused on IT risks for entities, escalate to an approach that analyses the risks for consumers and very specifically scrutinise the contracting process by digital means.
Technology outsourcing	In accordance with their specific regulatory set up, each supervisor may have to review, outsourced activities, including aspects like the complaint systems related to outsource services, the chain of outsourced providers and the concentration in a few of them.
SupTech	Technological development can enhance supervision through the incorporation of cutting-edge technologies into supervisors' procedures.
RegTech	Supervisors should keep up with regulation technology (RegTech) tools to understand them, evaluate their appropriateness, and interact with the industry to facilitate its development.
Innovation hubs and sandboxes	There is value for supervisors in considering whether to introduce innovation hubs and sandboxes to increase their understanding of financial innovation, its interplay with current regulatory frameworks, and to address changing market conditions in a timely manner. But these potential benefits must be carefully assessed against potential risks, taking into consideration the regulatory set-up of each jurisdiction.

CHAPTER 1: INTRODUCTION

1.1. Background

In the years since the financial crisis, financial institutions find themselves operating in an environment that has changed significantly on several fronts. They face greater regulatory requirements and shrinking profitability, while customers are changing their banking habits after losing confidence in the traditional players. Clients demand more customised products and are increasingly willing to interact with financial entities in a digital ecosystem. In this framework, technological developments in the field of digital financial products and services are providing opportunities for new services, new channels and new providers. Digitalisation is a significant contributor to this new financial landscape. Traditional financial entities must change their business models and keep pace with technological innovations to adapt to the new realities and to meet the new demands of their customers.

Digitalisation may bring many benefits to the financial system in terms of increased competition, efficiency and innovation, and new ways for customers to relate to financial agents. Properly used, the latter may help public confidence in the financial system to recover. For consumers, digitalisation may support a more consumer-centric experience, access to more financial services, greater choice, better prices and potentially more inclusive financial services, just to mention a few benefits.

Nevertheless, the risks to consumers that may emerge from this digital transformation are very significant. They include security issues, lack of consumer protection and lack of digital financial literacy. The financial sector may experience lower profits and/or engage in regulatory arbitrage; supervisors may identify defective compliance with regulation (anti-money laundering; counter-terrorist financing) or a lack of redress mechanisms.

Regulatory and supervisory authorities face huge challenges in this environment. As issues emerge in a fast-changing sector, they must move swiftly and provide up-to-date solutions, while simultaneously developing a deep understanding of a new and complex reality requiring the use of new analytic tools.

Even more, regulatory and supervisory decisions impact the development and implementation of new financial technologies (FinTech). Therefore, regulators and supervisors must adapt legal and supervisory frameworks to ensure supervised entities comply with regulation and, at the same time, to find ways to foster (or at least not impose undue burdens on) financial sector innovation.

Worldwide, the appeal of, and need for traditional brick-and-mortar banks providing in-person transactions is fast fading. In recent years, the G20, with the support of the OECD, has stressed the need to focus on the effects of digital transformation. In the same vein, FinCoNet has stated that the shift from traditional financial-sector delivery channels to online and mobile technology has important implications. These include supervisory authorities's ability to identify emerging consumer risks arising from digitalisation and to have appropriate tools to mitigate such risks. Consequently, FinCoNet Governing Council agreed[1] to include in FinCoNet's Programme of Work for 2017/2018 a new standing committee to develop further work on what has become this report, *Practices and Tools Required to Support Risk-based Supervision in the Digital Age*. FinCoNet, as a market conduct supervisory forum, is

[1] Decision taken during the November 2016 FinCoNet Annual General Meeting held in Jakarta, Indonesia.

in a privileged position to gain insight from its members and other authorities on the ways they are adapting supervisory tools to the challenges of DFPS.

1.2. FinCoNet focus on digitalisation

FinCoNet has paid special attention to digitalisation and the impact of technologies on the provision of financial products and services. The following are areas of special interest for this international organisation:

Supervisory toolbox and its adaptation to digitalisation

FinCoNet Standing Committee 1 compiled a database of supervisory tools used by FinCoNet members. These tools might be applicable to both traditional and digital financial products and services. This report, *Practices and Tools Required to Support Risk-based Supervision in the Digital Age,* could support the adaptation of this supervisory toolbox to meet digital challenges.

Digitalisation of short-term, high-cost lending: supervisory challenges to promote responsible lending

The growth of short-term, high-cost lending provided through digital channels has resulted in new challenges for supervisory authorities around the world. FinCoNet, through its Standing Committee 2 led by the Central Bank of Ireland, analysed this issue and in November 2017 released a final report focusing on the main supervisory challenges presented in this credit market. In 2018, FinCoNet is developing relevant guidance for supervisors in the field of digitalised short-term, high-cost consumer credit.

Online and mobile payments: supervisory challenges to mitigate security risk

The provision of payment services to consumers is changing rapidly, driven by technological innovation. To address this subject, FinCoNet's Standing Committee 3, led by Banco de Portugal, conducted the work on this subject. In September 2016, the committee released a report assessing regulatory and supervisory approaches adopted in this area titled *Online and Mobile Payments: Supervisory challenges to mitigate security risks*. FinCoNet Standing Committee 3 continues working on approaches and actions in response to the challenges identified in the first report. At FinCoNet's Annual General Meeting in November 2017, the committee presented its *Report on Online and Mobile Payments: An Overview of Supervisory Practices to Mitigate Security Risks*, published in January 2018.

1.3. Purpose of this report

The purpose of this report is to stimulate reflection among supervisory authorities on how to tackle the challenges stemming from the need to ensure proper consumer protection in the framework of new DFPS. For this reason, the report covers a wide range of issues, ranging from the institutional approach in terms of the supervisor's mandate, to an overview of the DFPS landscape among respondents, and the relevant risks identified and the supervisory tools used. The report covers the adaptation of traditional tools to digital needs, and the introduction of new tools such as innovation hubs or sandboxes.

The report, illustrated with practical cases and other examples of supervisory practices followed by authorities, contributes to the global FinCoNet goal of promoting cooperation among supervisors and sharing experiences. It should be noted that approaches identified in this report are regarded as effective in the context of the jurisdiction in which they were studied, and may not always be suitable to other jurisdictions. There is something to be learned from all approaches, even those deemed unsuitable for certain jurisdictions.

This report is based on the responses received to a survey questionnaire on practices and tools required to support risk-based supervision in the digital age. It takes stock of the various initiatives used by supervisory authorities to mitigate risks derived from the digitalisation of financial services. The survey was originally released to respondents during July and August 2017, and then the deadline for responses was extended to the end of 2017.

The survey collected information on relevant tools, practices, resources and processes used to identify and mitigate the risks and challenges associated with the provision of DFPS. The survey also covered the regulatory and supervisory landscape in the relevant jurisdiction in which the respondent authorities operate, as well as a review of the most relevant technological innovations in development in each jurisdiction, with identification of the risks associated with such activities. The survey included many open questions to allow respondents to explain concrete initiatives or experiences.

A total of 24 responses from authorities of 23 jurisdictions were received; 21 of these responses were from FinCoNet members. This includes central banks and financial service authorities. The 23 jurisdictions provide a global geographical representation.

1.4. Structure of the report

This report is organised in three main sections:

- **Overview of the digital financial products and services** (CHAPTER 2). This section includes an analysis of the regulatory and supervisory frameworks in which DFPS are being developed in the respondents' jurisdictions. It also includes a brief reference to the main initiatives in respondents´ jurisdiction with regard to the provision of DFPS, focused on the provision of banking and credit products and services; with a particular focus on the risks they pose.
- **Supervisory tools and practices to ensure risk-based supervision in the digital age** (CHAPTER 3), which identifies information about the supervisory tools used or that are being developed to mitigate the risks that result from providing financial products and services by digital means.
- **Innovation hubs and regulatory sandboxes** (CHAPTER 4), which gathers information about how tools such as innovation hubs and sandboxes contribute to regulatory and supervisory approaches.

All chapters set out the main findings from the survey responses, and Chapters 3 and 4 identify the most relevant case studies and supervisory practices related to the supervision of digital financial products and services highlighted in the survey responses. Finally, chapters 3 and 4 provide the main takeaways for supervisors.

The descriptions of supervisory challenges and approaches detected through the survey have been enriched using literature reviews and reports published by international financial organisations.

CHAPTER 2: OVERVIEW OF THE DIGITAL FINANCIAL PRODUCTS AND SERVICES

KEY POINTS

- Ensuring adequate regulatory and supervisory framework is essential in protecting financial consumers. Most respondents that have a mandate for "traditional" products are acquiring supervisory powers relevant to DFPS either from their regulators or they are extending their own mandates to cover such products. However, in many cases, adaptation of traditional powers and new rules are both required.
- The main principles guiding authorities are safeguarding financial stability and consumer protection. Technological issues and their impact in the financial sector are at the top of many supervisory authorities' agendas.
- To identify the potential risks of DFPS and to design effective regulatory and supervisory measures requires monitoring the digital products and services in development by industry in each jurisdiction, and across borders.
- Survey respondents identified the most relevant DFPS as home banking, mobile apps, crowdlending and peer-to-peer (P2P) lending, unsecured consumer credit and mobile wallets.
- The main DFPS-associated risks mentioned most frequently by respondents were: i) the lack of, or inadequate disclosure, information and transparency, ii) fraud risk and iii) the lack of, or inadequate data protection and privacy.

2.1. Regulatory and supervisory framework for DFPS

The first section of the survey focused on the regulatory and supervisory framework. This section was intended to identify the extent to which institutional and regulatory frameworks applied to "traditional" banking products, are also applicable to DFPS, and to assess whether these frameworks are considered suitable for meeting the challenges of supervising DFPS.

Institutional structure

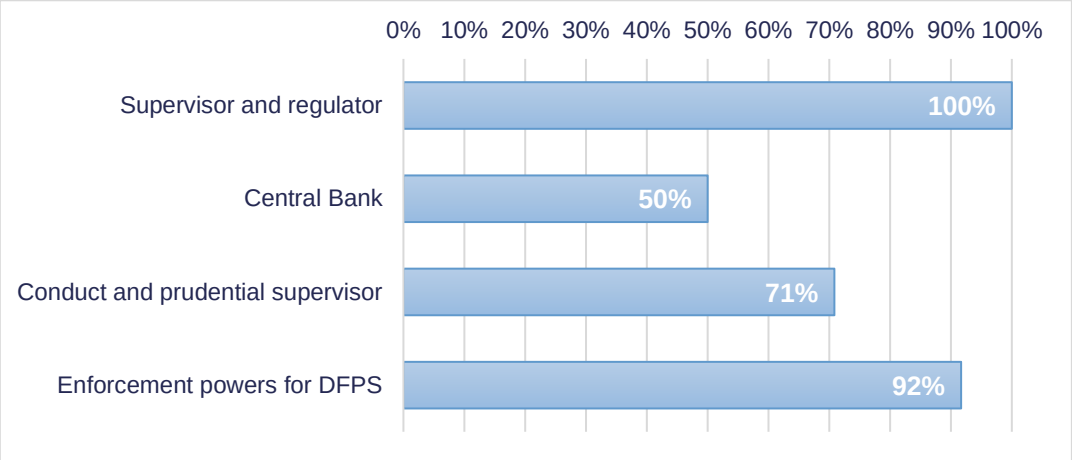
All authorities responding to the questionnaire are in charge of conduct supervision and consumer protection in their respective jurisdictions and have some level of regulatory powers. Regulatory powers over DFPS are normally allocated to the respective government body (ministry or department of finance) or parliaments, with some powers delegated to the central bank, supervisory authority or consumer protection authority. In most countries, the empowerment of competent authorities to issue regulation stems from the laws and regulations enacted by the government.

The majority of respondents said their competent authorities are in charge of regulation and supervision of financial product and services provided by supervised financial institutions, including DFPS.

Depending on the institutional model in a jurisdiction (twin peaks, sectoral, etc.), DFPS regulation and supervision may be shared between different authorities (prudential and

conduct authorities, banking, insurance and investment and securities authorities, etc.). This type of setup has implications in terms of coordination between all the authorities involved.

Graph 1 Respondents' profile

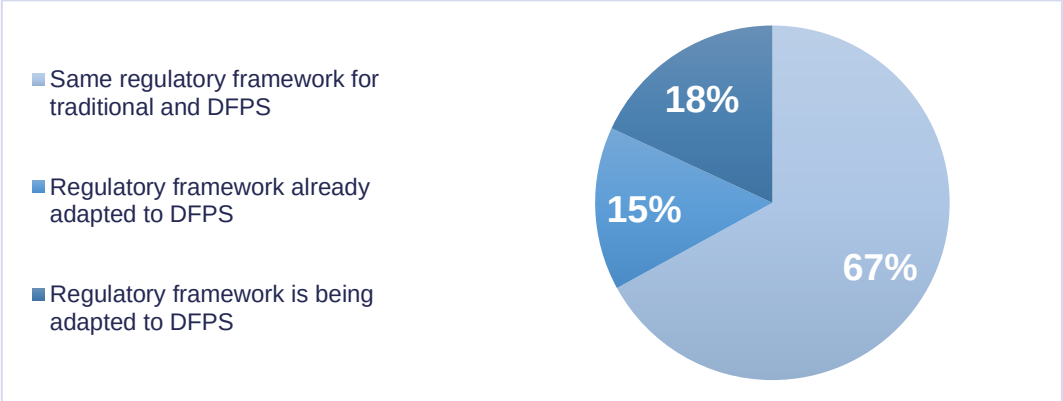


Regarding each respondent's profile, all have some form of regulatory and supervisory competences. Half are central banks and 71% are both conduct and prudential supervisors.

Current regulatory framework for DFPS

As can be seen in the graph below, only 15% of respondents said they have already adapted their regulatory framework to DFPS. However, this specific adaptation appears to be related only to certain products. Consequently, for the rest of DFPS, these authorities seem to be in a similar situation to the majority of respondents (67%) for which the applicable regulatory framework is generally the same for digital and traditional financial products and services. Several jurisdictions explicitly refer to "technology-neutral" regulatory frameworks or "principles-based approaches", with the same principles of regulation applying equally to digital and traditional delivery environments.

Graph 2 Regulatory framework



Although most countries essentially preserve the core of the regulatory framework originally designed for traditional products, in many cases, new rules and changes to existing rules are

being introduced to adapt to innovation and digitalisation of financial services, both to specific products and services or specific stages in the relationship with the customer (advertising, pre-contractual or contractual information, etc.).

Very few respondents referred to global adaptation of financial regulation. The Financial Consumer Agency of Canada (FCAC) refers to the Government of Canada's consideration of new and modernised legislation to address developments in products and services and the demands and banking habits of Canadians. The Central Bank of Ireland published a *Discussion Paper: Consumer Protection Code and the Digitalisation of Financial Services* about whether the code should be enhanced or amended in the face of innovative products. Other such as Netherlands Authority for the Financial Markets (Netherlands AFM) relies on a principles-based regulatory approach that alleviates the need to revise the framework to accommodate DFPS.

Table 2 provides examples of how some jurisdictions are adapting their rules concerning different products.

Table 2 Adaptation of rules governing DFPS

Country	Product/service	Implemented	In the process of implementation
Australia	Crowdfunding	X	
Brazil	Digitisation of paper documents related to financial transactions	X	
	Accounts through electronic means	X	
	Client identification in currency exchange contracts agreed upon electronic means	X	
	Crowdfunding	X	
	P2P lending	X	
France	Crowdfunding	X	
	Banking account aggregators	X	
	Digital subscription to financial products		X
	E-signature and registered e-mail		X
Germany	Crowdinvesting	X	
	Bank account opening via digital channels	X	
Indonesia	P2P lending	X	
Lithuania	Contracts concluded through distant communication	X	
Mauritius	Mobile banking and mobile payment systems	X	
	Digital payments		X
Portugal	Bank account opening via digital channels	X	
	Crowdfunding	X	
	P2P lending	X	
Romania	Digital payments	X	
Spain	Crowdfunding	X	
	Contracts concluded through distant communication	X	
	Digital payments		X

Indonesia OJK: P2P lending

Indonesia Financial Service Authority (OJK) recently enacted OJK Regulation Regarding IT-Based Direct Lending and Borrowing Services, specifically targeting P2P lending. FinTech P2P lending providers must comply with this regulation, while existing providers should comply with the existing regulatory framework.

As regards consumer protection aspects, providers must uphold five principles of consumer protection: 1) transparency, 2) impartial treatment, 3) reliability, 4) secrecy and security of consumer data and/or information, 5) simple, quick handling of consumer complaints and resolution of their disputes at affordable cost. P2P lending providers must give clear and honest information about their services, avoid the use of words that are misleading, and endeavour to ensure service offerings suit the client's needs and their ability to understand the service.

European legislation

For the 11 European Union (EU) jurisdictions that responded to the questionnaire, the rules defined in national legislation regarding retail banking products and services are, to a large extent, influenced by EU legislation. The European Commission, the European Parliament and the European Council elaborate EU Directives that must be transposed into national legislation, and EU Regulations that are directly applicable.

For example, this is the case of Payments Services Directive 2 (PSD2), where the European regulatory framework considers the recent developments in the sector. PSD2 provides opportunity to new actors (as opposed to banks, "payment institutions" and "e-money" institutions that are currently subject to a specific licence) to offer payment initiation services and account information services. These new actors are known as "third-party providers" and may be FinTech start-ups.

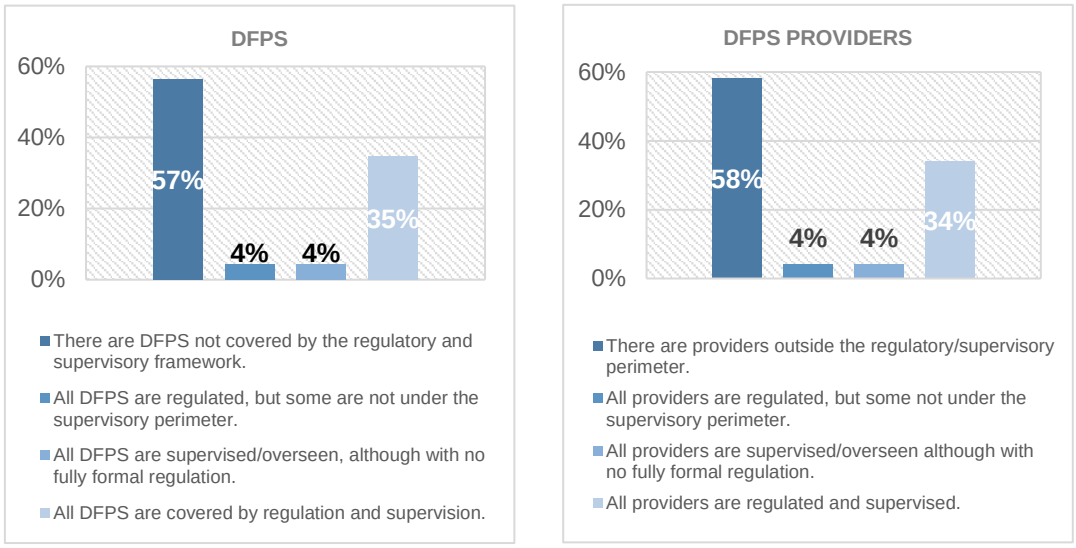
In adapting regulation to the digital era, there may be regulatory gaps affecting both DFPS and providers. Most respondents said some DFPS are not covered by the regulatory and supervisory framework of their jurisdiction.

With regard to DFPS providers not covered by the regulatory/supervisory framework, several jurisdictions generally referred to FinTechs such as data aggregator providers, online lending providers classified as non-deposit-taking institutions, cross-border DFPS (i.e. cryptocurrencies used as remittances), loan brokerage platforms, non-financial providers of digital/electronic payment instruments, and companies seeking to make use of initial coin offerings to raise funding.

In some jurisdictions there are DFPS that do not fit specific regulatory definitions, but they are somehow supervised inasmuch as they are provided by supervised entities or institutions. Although in over 30% of jurisdictions all DFPS providers are regulated and supervised, in most (58%) there are new agents providing DFPS outside the regulatory and supervisory scope.

Competent authorities are putting in place several measures to tackle gaps in non-regulated DFPS or providers. Among them are innovation hubs, analysed in chapter 4.

Graph 3 DFPS and DFPS providers



To adequately inform different agents about the regulatory framework, supervisory authorities are incorporating a variety of initiatives. Authorities such as BaFin (Germany) offer, on their website, a tool explaining the authorisation requirements applicable to specific DFPS models.

The Financial Conduct Authority in UK (UK FCA) has an advice unit providing regulatory feedback to firms developing automated models to deliver lower-cost advice, guidance or discretionary investment management services to unserved or underserved consumers. Firms that meet the advice unit's eligibility criteria will be given regulatory feedback on their model. This includes individual guidance, informal "steers" and signposting to existing rules and guidance. For example, an initial meeting is held to discuss the proposition, give specific feedback on the regulatory implications of the model and input on how to apply for authorisation, etc. The advice unit covers the following sectors: investments, pensions, protection, mortgages, general insurance and debt counselling. Firms with innovative models in sectors not covered by the advice unit can contact the FCA's innovation hub. A UK bank was the first firm through the advice unit and launched its automated investment advice model in November 2017, offering investment advice for a flat fee of £10. This compares with an average cost of £150 per hour for face-to-face advice.

In many situations, virtual currencies (VC, or crypto-currencies) are not considered subject to any regulatory and supervisory framework. In fact, various authorities have alerted consumers about the risks associated with VC use because they are neither regulated nor supervised. Jurisdictions that do not regulate crowdfunding have issued similar warnings.

In February 2018, the European Supervisory Authorities[2] (ESAs) for securities, banking, and insurance and pensions issued a joint, pan-EU warning to consumers about the risks of buying VCs. Moreover, individual EU countries have issued national warnings on cryptocurrencies. Outside the EU, Japan's Financial Services Agency (FSA) introduced a registration framework for broker-dealers of crypto-assets for legal tender. The FSA obliged such dealers to verify the users' identities and introduced provisions to ensure user protection, such as requirements regarding information disclosure, to users as of April 2017.

2 The European Supervisory Authorities (ESAs) are the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA).

In addition, warnings about the risks of crypto-assets (e.g. the risk of their high volatility) have also been issued to clients of crypto-assets broker-dealers.

The Australian Securities and Investments Commission (ASIC) has developed an information sheet (INFO 225) that gives guidance about the potential application of its *Corporations Act* to businesses that are considering raising funds through an initial coin offering. ASIC has also published information on its Moneysmart website providing guidance for investors about the risks of investing in initial coin offerings.

In Germany, BaFin has qualified VCs, with legally binding effect, as "financial instruments" in the form of "units of account" subject to the German Banking Act. As a result, BaFin may determine that, depending on the business model of a firm engaging in VC activities, it may be qualified to be performing a regulated activity under the national banking legislation (such as broking services or operation of a multilateral trading facility) that requires authorisation.

Enforcement powers

The vast majority of authorities have existing enforcement powers for "traditional" financial products and services that can also be applied to DFPS. The most common powers that authorities have available to enforce the regulatory framework (grouped by categories) are:

- **issuance of orders, recommendations, warnings, reprimands or notices**; these are used by authorities in different ways. They can be binding (typically orders) or non-binding (warnings or recommendations), and frequently depend on whether the institution is not in compliance with regulation or with best practices. The measures normally imply that an entity in breach of consumer provisions must take the measures necessary to comply with its obligations by a stated deadline.

- **administrative proceedings, sanctions, monetary penalties**: authorities may impose disciplinary sanctions and financial penalties in case of serious breaches or repeated infringements.

- **license revocation, business closure, disqualification of the person**: a temporary or definitive ban from performing one or several operations or activities, as well as any other restriction to the activity of the persons, such as disqualifying senior managers for a period.

Some authorities publish sanctions or specific decisions. One of them states that sanctions imposed will be disclosed to the public unless the disclosure would seriously jeopardise the financial markets or cause disproportionate damage to the parties involved.

Supervisory authorities' approaches to DFPS

According to the feedback provided, a number of authorities are still in the process of defining a strategic approach to DFPS. In doing so, safeguarding financial stability as well as consumer protection are by far the top priorities.

As can be observed in the table below, financial stability is the guiding principle most frequently referred to as the main priority by respondent authorities. This is coherent with the fact that a relevant number of the responding authorities are central banks. Consumer protection is also at the top of priorities and for some authorities, financial stability and consumer protection are considered to be of the same level of importance.

Other principles, such as promoting fair competition and innovation in the market, are considered important guiding principles too, although they may be perceived, in occasions, as difficult to conciliate with the principles of financial stability and consumer protection. While some authorities refer to the principle of "same business, same risks, same rules", others are afraid such an approach could limit innovation, thereby reducing industry competitiveness and consumer access to new digital products and services. Although innovation itself is not the main principle guiding the approach of any competent authorities, many are aware of the importance of digitalisation and take innovation into account in their strategy.

When UK FCA was created in 2013, one of its objectives was to promote effective competition in the interests of consumers. The FCA does three things to advance its competition objective. It looks at market structure and dynamics through its market studies, adjusting the "rules of the game" where necessary to improve consumer outcomes. It investigates anti-competitive behaviour under UK and EU competition law. And it implements regulation to support, rather than inhibit, competition in consumers' interests.

Table 3 Principles guiding the supervisory authorities' approach to DFPS

Principle guiding supervisory authorities' approach to DFPS	Rank				
	1	2	3	4	5
A) Innovation	2	2	7	3	2
B) Fair competition	1	4	3	3	2
C) Financial stability	14	1	2	1	3
D) Consumer protection	10	7	1	-	-
E) Financial inclusion	-	2	4	5	5

Table: Number of times the rank was selected for the respective principle, with 1 being the main guiding principle.
The table reads as follows: With regard to consumer protection, 10 respondents assigned rank 1, 7 respondents assigned rank 2, 1 respondent assigned rank 3 and no respondents assigned ranks 4 and 5. Not all respondents considered all ranks/principles.

Finally, aspects related to financial inclusion still appear to be relevant for a number of respondents, but of minor importance compared with the aforementioned aspects.

Regardless of the priorities, most authorities have incorporated technological issues in the agendas of their top bodies. Some authorities, such as the Bank of Lithuania and the Autorité des marchés financiers du Québec (AMF) in Canada have established long-term strategic plans (2017-2020) to address the regulatory challenges brought on by new technologies. Other authorities, such as the relevant supervisory authority in Luxembourg, Brazil, Portugal and Spain, have set up or are involved in working groups to improve their knowledge of FinTech and DFPS and to assess the consequences of technological innovation.

Idiosyncratic factors

To better capture the impact of DFPS from a regulatory and supervisory perspective within their jurisdictions, competent authorities consider idiosyncratic factors of social, cultural, demographic, technological, financial or legal nature. This may explain specific aspects of DFPS development in each jurisdiction and the corresponding supervisory approach. Indeed, as shown in the responses received, there is no a single driver; rather, there is a range of relevant factors that seem to be strongly correlated with each other. Even though determinants may be country-specific, a number of similarities can be observed.

- **Social factors** affecting the population's tendency to use digital channels. Some authorities refer to the internet's high market penetration and the growth of

smartphone and tablet use, together with better informed and more demanding consumers. Other jurisdictions point to customers who seem reluctant to use digital channels and consequently tend to choose traditional banking products and face-to-face commercial relationships.

- **Demographic factors:** the trend among entities to close banking offices, especially in less densely populated or remote areas due to declining local population, has led people to use digital financial services to replace those formerly provided by a local branch.

- **Geographical factors**: barriers that strongly limit or restrict the availability of optical-fibre networks or mobile broadband internet access.

2.2. Most relevant DFPS and the risks they pose

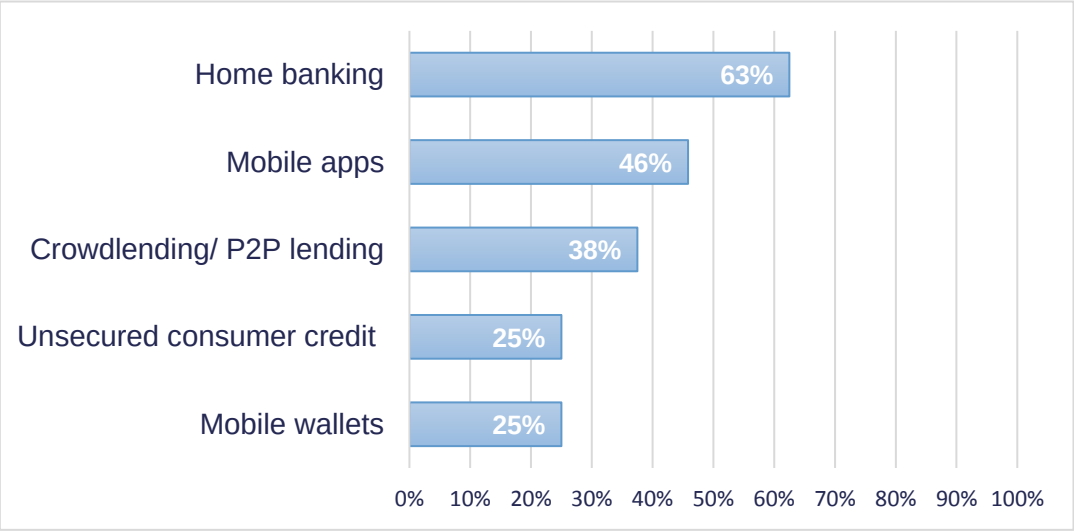
Supervisors are challenged in determining the full landscape of DFPS in development at any time. This is due to the speed of technological change and to the fact that many developments fall outside the financial regulatory framework. Despite the difficulties, supervisors need to understand the DFPS activities emerging in their jurisdictions in order to identify the risks they may pose to the system and to customers, and adopt the appropriate regulatory and supervisory measures.

Survey respondents were asked to describe the most relevant DFPS in development in their jurisdictions and the type of related risks of most concern to them.

Most relevant digital financial products and services

The following graph shows the aggregate responses to the survey request to “select the three most relevant digital financial products and services developed in your jurisdiction from the list below”. Each authority identified three DFPS, and the graph shows the percentage of authorities mentioning those DFPS.

Graph 4 Most relevant DFPS



Home banking and mobile apps allow customers to check account balances, view bank statements, make credit transfers, transact payments through online platforms (internet banking) and mobile devices (apps), and contract products and services. This technology seems to be mature in most countries, and is one of the channels preferred by consumers.

A number of respondent authorities selected crowdlending and P2P lending: in some cases, authorities supervise crowdlending platforms.

Unsecured consumer credit was mentioned by a quarter of authorities and deserves special attention because it can encourage over-indebtedness. DFPS has the potential to facilitate quick, easy and user-friendly access to credit. Consumers may also value the anonymity and impersonal nature of borrowing through digital channels. This practical accessibility may bias consumers to demand more credit than they need and, even worse, than they can repay. As mentioned above, such irresponsible lending could lead to a state of over indebtedness.

Mobile wallets have also been mentioned by 25% of the authorities. The survey's list of DFPS did not include "mobile payments" as a general category; instead, it included a list of single DFPS that, taken together, could be considered mobile payments. As a consequence, the table above may underestimate the relevance of mobile payments, as 83% of respondents selected at least one of the following DFPS as the most relevant: mobile wallets, card not present, mobile third-party payments, virtual cards, payments by short message service (SMS), online wallets, and direct mobile billing. Most case studies provided in this context referred to companies that enable mobile payments and/or transfers.

Most relevant risks

Table 4 below defines each risk category associated with DFPS, followed by graph 5 showing how survey respondents prioritise each risk category.

Table 4 Relevant risks associated with DFPS

Lack of, or inadequate disclosure, information and transparency
• biased, incomplete or misleading advertisement • lack of adequate framework (e.g. devices) for pre-contractual information analysis • lack of consumer understanding of product characteristics or service terms and conditions, due to complicated and lengthy user agreements; unclear pricing, fee and exchange rate structure; and inadequate environment to assess complex information • contract changes made unilaterally by service provider • abusive clauses
Fraud risk
• unauthorised account opening (identity theft, contractual capacity) • unauthorised access to consumer accounts and funds/unauthorised transfer • internal fraud, authorised agent fraud • risk of new scams • money laundering and terrorist financing
Lack of or inadequate data protection and privacy
• use of financial data by third parties • data breaches • problems in the treatment of personal data (also cross border)

Consumer risks resulting from technology problems
• inability to operate and access funds (no business continuity, systems unavailable) • market fragmentation–interoperability restricted • insufficient operational capacity–slow response time • general security standards—unable to withstand hacking • general system errors–poor consumer experience/loss of funds
Limited consumer protection and recourse
• dilution of responsibilities when many companies are involved • inexistent or inaccessible complaints channels (at provider's level or by way of alternative dispute resolution) • lack of transparency in complaints handling • lack of response in a timely manner (complaints "black hole") • limits to dispute resolution, mandatory internal forum or arbitration agreement • shortage of cross-border service providers, or difficulties in having to litigate in another country under foreign laws • consumer misunderstanding, lack of awareness regarding their right to complain
Poor outcomes for consumers
• over-indebtedness • lack of clarity concerning intermediaries' responsibilities • service-provider failure or insolvency • financial exclusion/ethical discrimination/big data bias

In addition to the list above, respondent authorities identified other DFPS risks that the questionnaire did not cover explicitly. Among these, respondents highlighted the possible risk of financial exclusion.

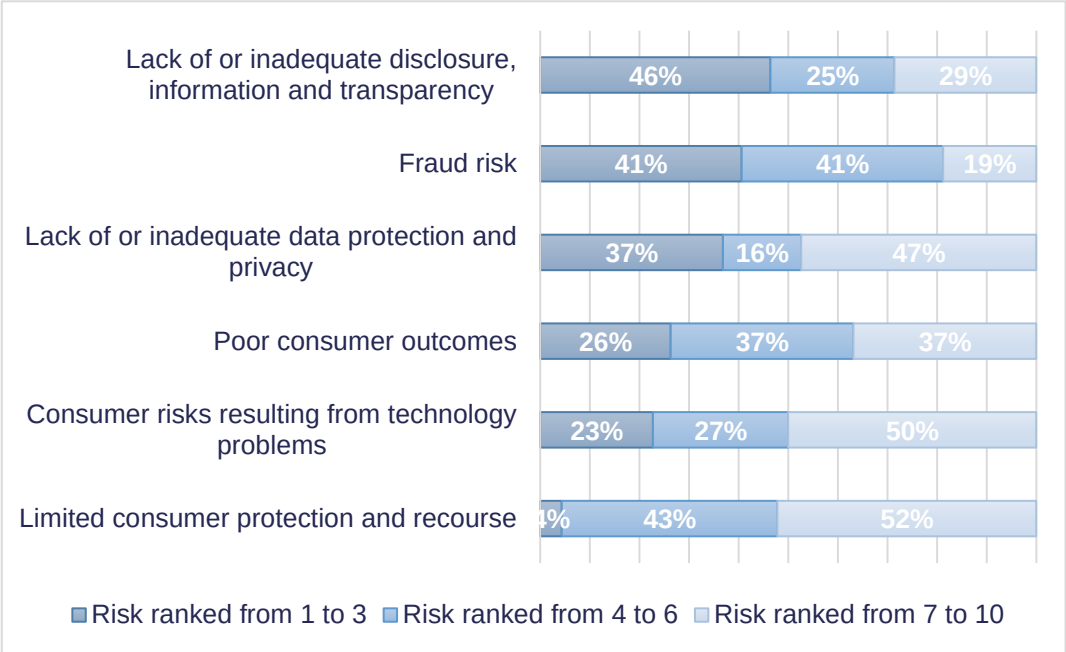
Without adequate precautions, DFPS may, on the one hand, restrict some consumers' access to products and services that had been available to them through traditional means. This may be particularly true for consumers who are not technologically literate or have limited or no access to modern technological devices (digital barrier). Second, low levels of financial and digital literacy may increase exclusion. User-friendly digital environments may make it all too easy for consumers to handle DFPS carelessly. For example, consumers might conclude credit contracts thoughtlessly; should they end up in default, they may be excluded from access to financial products and services. Finally, new kinds of exclusion could arise when digital profiling based on artificial intelligence and data-driven algorithms are used by the financial sector to make credit decisions.

On the other hand, DFPS offer consumers customised and inexpensive solutions; providers benefit from cost-efficient design. DFPS are expected to expand public access to financial services and products, especially for unbanked people.

On balance, DFPS seem to have a huge potential to increase financial inclusion but some respondents warn the opposite is also possible. To address the latter possibility, respondent authorities are developing financial education materials, including videos specifically designed for vulnerable groups of people on how to use DFPS properly.

Using the definitions in table 4 above, respondents ranked each risk from 1 to 10 according to its importance, with 1 being the most relevant risk; the results are below in graph 5. Each product and/or service presents a different set of risks for regulators and consumers and therefore might imply different potential concerns and challenges.

Graph 5 Prioritisation of relevant risk categories associated to DFPS



CHAPTER 3: SUPERVISORY TOOLS AND PRACTICES TO ENSURE RISK-BASED SUPERVISION IN THE DIGITAL AGE

KEY POINTS

- To ensure adequate consumer protection, authorities are creating and/or adapting supervisory tools and techniques to address the risks derived from DFPS commercialisation. For this reason, many authorities have created internal multidisciplinary working groups to understand DFPS particularities and adapt supervisory tools as needed. The main challenges supervisory authorities face when supervising DFPS are lack of technological expertise, regulatory gaps and cross-border issues, and difficulties addressing these swiftly, to keep up with changes to DFPS.

- Off-site surveillance tools most frequently used to supervise DFPS are: regular meetings with financial providers, specific questionnaires, ad hoc information requests and thematic evaluations on DFPS provider functions. The same warning indicators used to anticipate risks related to traditional products are used for DFPS, although new approaches, such as social-media monitoring and whistleblowers, are in implementation. Complaints handling and data reporting also are being adapted to capture granular data that may give statistical support to supervisors.

- On-site inspections can be complemented by using remote access to supervised institutions' technological platforms and by using technical expertise to design new supervisory tools. Supervisors must be able to reproduce the client's interaction with DFPS. Additionally, on-site inspections should focus on new matters such as institutions' IT systems, cybersecurity, product and services developments and thematic reviews on cloud storage, robo-advisors, P2P, etc.

- Keeping up with emerging DFPS and other technological changes requires increased recruitment of experts in digital technology who would help adapt tools. Cooperation among national and international authorities in the field of DFPS enhances authorities' DFPS knowledge through formal and informal means.

3.1. Adapting traditional tools to the digital world

Supervisory authorities are at different stages in adapting to the challenges digitalisation implies for their supervisory activity. They need to understand the digital phenomenon in order to design appropriate supervisory tools. Consequently, the progressive response of many authorities is based on an initial application of traditional supervisory tools to DFPS, to identify, in a second step, whether there is a need to adapt such tools to address DFPS, and to finally produce brand new tools dedicated to DFPS where needed.

Traditional tools

The survey shed some light on:

- whether traditional tools to supervise traditional banking products are being used (or there is an intention to use them) to mitigate DFPS risks
- whether this new use of traditional tools is proving successful
- the initiatives underway to adapt traditional tools or create new ones

Table 5 shows the extent to which respondent authorities resort to traditional tools.

Table 5 Supervisory tool or practice

Supervisory tool or practice	Traditional financial products and services used	Digital financial products and services	
		In use	Intend for use
Cooperation with other authorities	23	20	3
Issuing guidelines	22	16	6
Licensing and authorisation	22	16	6
Off-site surveillance	22	15	6
Complaints handling	23	20	3
Data reporting	24	16	9
On-site inspection	23	16	7
Financial education	17	14	2
Mystery shopping	8	3	3
Moral suasion	15	11	3
Enforcement	24	19	5
Sanctioning powers	24	19	4
Redress powers	9	7	2

According to the information above, authorities rely, to a great extent, on traditional tools in supervising DFPS. In most cases, when these tools are not yet in use with DFPS, the supervisory authority intends to use them in the future. In fact, the use of these tools seems to be the result of the practical approach that consist of extending the tools already applied for traditional products to DFPS, especially in those cases in which the possibility to apply different tools is not foreseen in the legislation.

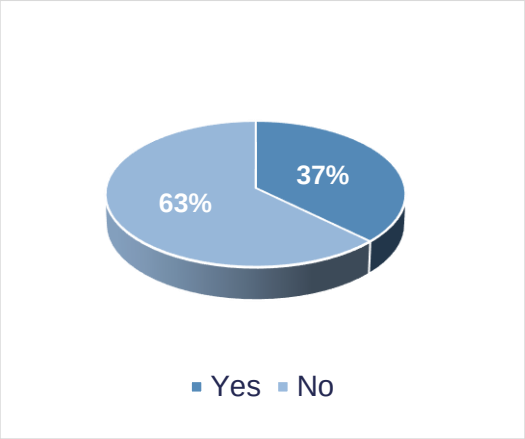
Some respondents said they have not undertaken any significant consumer protection supervisory work explicitly in relation to DFPS. Others stated that they have no DFPS-specific supervisory measures or powers in their jurisdiction, but that DFPS providers can be subject to the whole range of measures at their disposal. This does not mean that practices and tools are applied to DFPS in exactly the same terms as they are to traditional products.

Are traditional tools adequate?

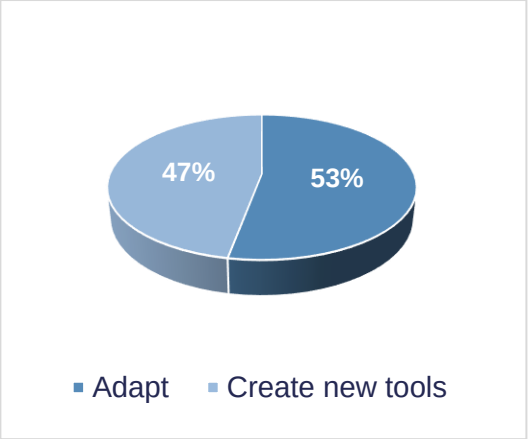
When asked about the effectiveness of traditional tools into protecting consumers from risks related to DFPS, most of the authorities answered that these tools are neither adequate nor sufficient to protect consumers. As graphs 6 and 7 show, respondents indicate that traditional tools must be adapted or new tools created to address differences between digital and traditional products and channels. In the same way, they understand that supervision must be flexible and dynamic, while consumers must be educated about these new products and their associated risks.

The following graphs show respondents' views with respect to the sufficiency of the traditional tools in addressing DFPS risks. Most of the respondents think that traditional tools are not adequate to ensure sufficient consumer protection. While about half of those respondents consider the adaption of traditional tools to be sufficient, the other half refers to the creation of new tools.

Graph 6 Are traditional supervisory tools adequate and sufficient to protect consumers from risks related to DFPS?



Graph 7 If no, would it be sufficient to adapt traditional supervisory tools or should new supervisory tools be created?



Therefore, it could be concluded that, in general terms, supervisory tools indicated in table 5 above may be adequate for supervising DFPS, while some would need adjustment, changing the techniques and procedures used to supervise traditional products and services. The tools in table 5 are general tools that may be applied in very different ways depending on the techniques used, and the purpose of the application of such tool. For example, an on-site supervision visit may be used to supervise both traditional products and DFPS; nevertheless, some techniques applied in such visits are necessarily different.

In this regard, traditional supervisory tools (such as onsite inspections, offsite surveillance, sanctioning powers) do not necessarily need to be radically transformed for use in relation to the digital revolution. However, the way they are implemented may have to evolve and will require the use of new IT tools and a broader range of supervisory expertise.

Challenges in DFPS supervision

Conduct supervisors face many challenges concerning the supervision of DFPS. Some are inherent to their mandate of consumer protection. Other challenges are very much linked with the process of adopting the appropriate supervisory tools.

Table 6 Challenges and difficulties in DFPS supervision

Challenges and difficulties	Number of authorities
Lack of adequate technological expertise Keeping staff up to date	16
Changing environment	9
Regulatory gaps Unregulated entities	8
Lack of statistics	5
Lengthy approval process for new legal regulation, may impact financial consumer protection	4
Cross-border issues	4

Supervisory authorities responded that the main challenges they face are related to the need to incorporate technological expertise to keep up to date with the changing environment and to adapt their current regulatory set up (regulatory gaps, cross border issues). To make it

more challenging, both aspects may have to be adapted in a swift manner, as digitalisation issues change so fast. The speed of technological innovation contrasts with the lengthy timeframes needed for recruiting the appropriate staff, understanding new needs and approving new regulation. Supervisors need to recruit staff with high technological skills and keep the current staff up to date.

Respondents also identified limitations in their regulatory set-up. Among them, they mention the absence of regulation of some activities or the fact that the actual legal and regulatory environment does not fully consider digital aspects. Regulatory gaps may allow some unregulated companies to perform activities traditionally carried out by regulated entities. Some supervisors also mentioned they lack adequate powers to enforce consumer protection when products/services are supplied across borders by foreign-based providers.

Other challenges relate to the lack of statistical information for use in determining the significance of new businesses and to monitor them (number of customers, distribution channel, geographical area of operations, etc.). This shortage of standardised and periodic DFPS information makes it difficult to develop supervisory tools and assess potential risks.

In the same vein, in February 2018 the Basel Committee on Banking Supervision published a report on *Sound Practices on the Implications of FinTech Developments for Banks and Bank Supervisors*. Similar to this report, the Basel committee identified the need to reassess current supervisory models and resources, specialty training programmes for current staff and the addition of specialised staff.

3.1.1. Internal working groups

Many supervisors referenced the creation of specific working groups to handle the challenges described above. These groups analyse the business models used by DFPS providers, including FinTech companies, plus DFPS features and their associated risks. They then design the regulatory and supervisory responses to such risks.

Table 7 Fostering digital adaptation–internal working groups

Country	Name	Task and composition
Peru	FinTech Working Group	Exploratory research in 2017 to identify business models that have been emerging in the Peruvian marketplace and to recommend actions towards each one. Departments of Technological Risk Supervision, Operational Risk Supervision, Banking Supervision, Insurance Supervision, Market Conduct Supervision, Regulation, Legal Advice and Economic Research.
Spain	Financial Innovation Group	Analyse the new trends; help define the Banco de España's DFPS strategy; coordinate the actions of different departments and with other authorities. Representatives of different areas: technology, prudential supervision, conduct supervision, payment systems and financial stability.
	Associate Directorate General	Banco de España has also recently created a new Associate Directorate General Financial Innovation and Market Infrastructures with the aim of monitoring and analysing financial market innovations.
Brazil		Assess the consequences of technological innovation on the provision of financial products and services.
Portugal		Analyse possible scenarios for strategically positioning the Banco de Portugal regarding FinTech and digital banking: (i) facilitator (i.e., to observe actively, and promote dialogue with stakeholders; (ii) catalyst

		(i.e., to intervene with the aim of encouraging financial innovation; and (iii) accelerator (i.e., to participate actively in the cycle of financial innovation). Keep track of developments in financial innovation, assessing the impact of digital transformation in terms of internal organisation and processes.
Netherlands		The mandate is to ensure that the Netherlands AFM accommodates technological innovation that is in the interest of consumers and investors, while simultaneously addressing the risks related to these innovations. The team interacts closely with market participants (e.g., via the innovation hub) and cooperates with other departments within the Netherlands AFM and participates in various international working groups. The team produces warnings (VCs and initial coin offerings, the impact of artificial intelligence (AI) on financial services, or digital marketing) and organisational changes regarding setting up a dedicated team responsible for IT governance, or influencing the strategic priorities of the Netherlands AFM. People with different backgrounds, i.e. IT, legal, strategy consultancy, capital markets experience.
Canada AMF	FinTech Working Group	Analyse technological innovations in the financial sector and anticipate regulatory and consumer protection issues; analyse and make recommendations about the ability of the current regulatory framework to support changes in commercial practices, business models and financial sector technologies while ensuring a solid balance between consumer protection and market efficiency. Exchange with industry and consumer groups to better understand their concerns.
Germany	BaFin's innovations in financial technology unit	The unit is responsible for the identification and impact assessment of selected technology-driven developments of strategic importance for the financial market. It develops possible future scenarios in regard to the effects of financial technological developments, as a basis for the authorities´ strategic positioning, advises the divisions and management on specialist inquiries and on further regulatory development concerning financial technological developments. To this end, BaFin's innovations in financial technology unit bundles, analyses and networks internal and external information as well as knowledge and decision makers and enriches them with its own know-how. The unit closely interacts with all relevant divisions of BaFin and Deutsche Bundesbank.

Takeaways

Respondent authorities identified the use and/or adaptation of traditional tools, and the engagement of multidisciplinary working groups, as two particularly useful ways of ensuring supervision keeps up to date with technological development.

Adaptation of traditional tools	Traditional tools may be applicable to DFPS supervision, but some adaptation may be needed, using techniques and procedures incorporating the technological dimension.
Internal steering groups	The creation of internal multidisciplinary working groups (supervision, legal, IT, anti-money-laundering (AML), etc.) can be helpful to gain better understanding of DFPS and determine the supervisory tools to apply to them.

3.2. Off-site surveillance

Respondents identified various types of surveillance activities performed in the area of DFPS:

Table 8 Off-site activity

Off-site activity	Number of authorities
Specific reviews	12
Regular liaison meetings	9
Questionnaires and ad hoc information requests	7
Thematic evaluations of different DFPS provider functions or departments	7

Several authorities said they had not developed tools for off-site DFPS surveillance. Off-site activities are carried out at a general level (traditional approach); although DFPS are in the scope of these activities, they are not specifically designed for them.

As seen in the table above, supervisors perform different types of specific reviews of files of information, advertising, pre-contractual and contractual information, ad hoc reporting, etc. One of the most frequent, simple and effective tools is holding regular meetings with financial providers. Questionnaires and ad hoc information requests have also been identified as a main off-site activity. Some countries also use thematic evaluations on DFPS providers' functions or departments to assess compliance with legal requirements.

Some authorities have schemes in place to analyse, and sometimes to approve new products. For this purpose, they maintain a database with all these products and their features. These schemes give the supervisor visibility on relevant developments that are taking place in the market.

Some respondents categorise the risk assigned to each (regulated) entity (conduct risk profile). Nevertheless, these risk indicators barely cover attributes related to DFPS due to the lack of reliable, standardised, periodical data related to digital aspects.

3.2.1. Questionnaires and research

To obtain an in-depth knowledge of the digital reality affecting their competences, some authorities have followed a similar approach, which consists of issuing to their supervised entities a questionnaire to illustrate the DFPS phenomenon, to measure the main risks associated with DFPS and to adapt DFPS regulation and supervision. Various authorities indicate they are currently carrying out industry surveys or are planning to do so. These questionnaires are normally conducted as one-off exercises to gain insight into the DFPS market at a given point in time, rather than on a periodic basis. For example, some authorities, such as the Central Bank of Ireland and Banco de Portugal, have developed specific surveys/questionnaires. Examples are below.

Central Bank of Ireland: research on digitalisation of financial services[3]

The Central Bank of Ireland issued a survey to regulated firms seeking information on the new and innovative products and services that have been offered or are in development in the Irish consumer market in the digital financial services context.

The main objectives of this research were to identify:

- innovative solutions introduced to traditional processes to date
- product areas impacted by each innovative solution
- innovative solutions that firms planned to introduce to traditional business processes in the next 12 months
- high-level details for each innovation-related initiative adopted to date
- innovations that were to be in development in the next 12 months
- high-level details of firms' innovation hubs

This research was conducted through a web-based survey of 21 regulated firms, representing the main financial-sector players, across five sectors (banking and insurance industry, investment firms, payment/e-Money institutions and retail intermediaries). The bank conducted the survey to inform the content of its *Discussion Paper: the Consumer Protection Code and the Digitalisation of Financial Services*[4]. The paper assessed how the code addresses emerging risk from digitalisation and whether the existing protections need to be enhanced or adapted in specific areas.

Banco de Portugal: questionnaire on commercialisation of banking products and services through digital channels

In 2016, Banco de Portugal sent banking institutions a survey about the digitalisation of retail banking products and services[5]. The main goals were (i) to gain detailed knowledge of financial institution practices in marketing banking products and services on digital channels and (ii) to assess the existing obstacles to digital channel development, on both on the demand and the supply sides, with particular attention to any constraints in terms of the legal and regulatory framework.

As a consequence, Portuguese law has been amended to allow customers to open bank accounts exclusively via digital means, which implies that client identification and authentication are being conducted by videoconference.

Takeaways

Effective supervision and monitoring depend on obtaining information on the products marketed through digital channels, the entities that provide them, their respective characteristics, the specificities of the contracting process and the security mechanisms.

[3] http://www.centralbank.ie/docs/default-source/publications/consumer-protection-research/industry-research-on-the-digitalisation-of-financial-services.pdf?sfvrsn=8
[4] https://www.centralbank.ie/docs/default-source/publications/discussion-papers/discussion-paper-7/discussion-paper-7-digitalisation-and-consumer-protection-code.pdf?sfvrsn=0.pdf?sfvrsn=0
[5] (https://clientebancario.bportugal.pt/sites/default/files/relacionados/publicacoes/QuestCanaisDigitais2016_EN.pdf)

Questionnaires and research	Asking a wide representation of the key players in each jurisdiction to respond to a comprehensive questionnaire may provide insight on the main risks posed by DFPS and determine the possible need for measures to safeguard the interests and rights of consumers.

3.2.2. Early warnings

Early warning tools and risk indicators help identify the main risks for consumers. The majority of respondents indicated they assess the same warning indicators to anticipate new DFPS risks as they would for traditional financial products and services. Nevertheless, some countries have developed risk indicators specifically related to these products. Some have created dedicated teams to undertake this work. The table below summarises the main early warning tools used by the competent authorities to anticipate new risks related to DFPS.

Table 9 Early warning tools/risk indicators

Early warning tools/risk indicators	Number of authorities
Social media monitoring, news media monitoring, and other industry research and questionnaires	11
Complaints	8
Data reporting	8
Internal risk-assessment workshops, other internal teams and self-assessment tools	4
Meetings with entities, information from entities about new products, entities' webpages	5
Information from on-site inspections, operational risk reports	3
Participation in international fora	3

As per the table above, nearly half the respondent authorities said their early-warning tools in monitoring financial market developments are: social media monitoring, online monitoring, press reviews, interviews with consumer representatives and other industry research, and questionnaires.

Social media and other online monitoring provides information on new DFPS, innovative and disruptive developments and identify trends in consumer dissatisfaction with products and services. While the external information analysed with this tool is not standardised, its review will provide a barometer of public opinion and potential consumer issues, with high potential to alert supervisors about emerging risks. Precisely for this reason, this tool has the capacity to help supervisors explore beyond the borders of regulated DFPS.

Similarly, other authorities operate a consumer helpline and have set up a central contact point for whistleblowers.

Other early warning tools mentioned by authorities include information:

- obtained in day-to-day supervisory activity, such as meetings with entities (specifically information about new products)
- from on-site inspections
- from external auditors

- from reviews of entities´ webpages, operational risk reports and incident reporting schemes

Some respondents pointed out that systemically important financial institutions (SIFIs) are subject to continuous monitoring by supervisory authorities; this can foster discussions on new products (i.e. online account, digital services) prior to their launch, in order to avoid any non-compliance with regulations.

The close contact with industry and stakeholders is an important early-warning tool. The Financial Consumer Agency of Canada (FCAC) holds meetings, both ad hoc and scheduled, with regulated entities and other stakeholders. These are important in monitoring and promoting compliance with federal consumer-protection provisions, and in staying on top of emerging trends and concerns regarding consumer protection. These meetings include:

- annual “Industry Sessions” at which the Agency advises mid-level and senior bank staff about its concerns and compliance actions
- regularly-scheduled meetings with a broad array of consumer groups and financial-industry specialists such as academics, to keep them informed of FCAC efforts to protect consumers and hear from them about emerging trends and concerns
- the financial literacy team’s ongoing engagement with a broad array of Canadian interest groups, including through its national steering committee, its research sub-committee and its national working groups

One indispensable early-warning tool is participation in international fora. In a globalised world where entities want to provide products and services across borders, authorities can share experiences at these gatherings on the main issues. This aspect is developed in 3.4.1.

To design regular and reliable early-warning tools, two sources of information are especially important as long as authorities receive them through formal channels: complaints handling and data reporting. These tools will be analysed in the following points of the report.

Some examples of early warning tools and risk indicators follow.

Central Bank of Ireland: gathering data on consumer experiences by monitoring social media and other online trends

The Central Bank of Ireland began monitoring social media and other online platforms in 2013. The procedure consists of monitoring publicly available social media platforms, blogs and online content such as web pages and fora against a list of approximately 50 key words. A “mention” is recorded if the keywords are matched. This word list is updated regularly and includes references to various financial products and services in addition to a list of financial services firms active in the Irish market.

The information obtained (such as expressions of dissatisfaction and general conversations highlighted by the tool) is used to prepare reports categorised by topic, firm name, product sector and social media channel and to assess risks facing consumers and shape the consumer protection priorities and agenda. It is a valuable source of information for risk analysis, policy formulation and supervision.

The indications provided by social media activity have supported the Central Bank of Ireland in challenging firms on the concerns raised by their customers; enabled supervisory interventions, resulting in a firm hiring more customer-facing staff; and have resulted in the central bank issuing public warnings.

France's ACPR: outsourcing solutions

In France in 2016, l'Autorité de contrôle prudentiel et de résolution (ACPR) put in place two tools to strengthen its watch on products and business practices. The objective was to complement ACPR's traditional ways of monitoring the market. These two new tools are used to establish quarterly internal reports.

- **Innovation watch:** ACPR uses this tool to follow banking and insurance innovation. The innovation watch is outsourced. The ACPR has access to a service that gathers information about innovation. This solution is provided by a French firm, whose clients include significant French insurers and bankers. Information is classified by type of service and product, with a brief analysis of how each DFPS is innovative, and which firm is leading its development and which one(s) is a mere follower. Data is mainly based on an exhaustive gathering of public news releases.
- **Listening to social media:** this tool is based on an external IT solution, too. It is used by a number of firms to monitor their public impact and reputation or the impact of their internet communications. The process consists of identifying a topic of interest and listing keywords to create an accurate query (relevant keywords, words, websites and expressions to exclude). "Noise" such as advertisements, job openings and other irrelevant material turned up in the search are removed and the remaining results are reviewed. Finally, remaining messages are categorized under specific topics and sub-topics on the basis on pre-defined keywords and statistics.

Some authorities have initiatives to boost citizens' communications with the supervisor, to provide specific information. This is typically the case of whistleblowing.

UK FCA: handling information from whistleblowers

The Financial Conduct Authority in the United Kingdom (UK FCA) uses a very wide range of information sources in their work and whistleblowers provide valuable intelligence on both criminal and regulatory breaches, as well as on general wrongdoing in the regulated sector. UK FCA protects the whistleblower's information and identity unless they choose to disclose their identity to the firm concerned.

In many instances, a whistleblower's information simply corroborates intelligence already in UK FCA's possession, or is new but not new enough on its own to warrant further action. Still, it may draw attention to a potential risk. Sometimes UK FCA uses the whistleblower's information, pieced together with information from other sources, to take action.

Information from whistleblowers has contributed the authority's actions against firms and individuals, including fines, withdrawal or changes to permissions, warning letters and a range of other early interventions, such as asking a firm to clarify its activities. UK FCA has also used information from whistleblowers to inform their supervisory strategy.

The Australian Securities and Investments Commission (ASIC) has a dedicated process to receive, handle and process reports of misconduct from consumers, industry participants, industry associations, other regulatory agencies, and ASIC-approved external dispute resolution schemes. Further, Australian Financial Services (AFS) licensees must notify ASIC in writing of any "significant" breach (or likely breach) of legal obligations. Although this feature is not DFPS-specific, they are also covered. ASIC also has a primary role in relation to whistleblowers, assessing and (where appropriate) investigating disclosures. ASIC also looks into misconduct relating to allegations that whistleblowers have been victimised for making a protected disclosure.

Takeaways

Supervisors use a wide range of tools for off-site surveillance that could be applied specifically to DFPS.

Close contact with industry and stakeholders	Regular bilateral meetings and other means of keeping regular contact with supervised entities and other stakeholders can keep authorities informed of DFPS developments and enable their detection of worrisome issues. In addition, a valuable input can be obtained from regular meetings with DFPS providers. Other relevant stakeholders may include academics and consumer representatives.
Social media monitoring	Monitoring the mass media and social media may help supervisors to remain up-to-date on new products and emerging risks.
Consumer helpline and whistleblowers	The different schemes to allow whistleblowers to inform supervisors of inappropriate conduct by supervised entities can provide valuable, up-to-date information, particularly in the rapidly changing digital environment.

3.2.3. Complaints handling

Complaints are a crucial indicator of the relevant risks associated with a product or service. Complaint statistics are a powerful source of information for risk-based supervision. Many authorities categorise complaints by type of product, object of the complaint, financial service provider, etc. Although complaints handling is still oriented toward traditional products, the use of DFPS-specific codes to support identification of emerging issues related to digital products is being introduced increasingly by complaints handling services.

Takeaways

Complaints handling	Introducing specific codification in the complaints categories to allow the identification of DFPS issues may create a high-potential tool for monitoring and early warning.

3.2.4. Data reporting

Most respondents receive a range of financial regulatory reports on a daily, monthly, quarterly and semi-annual basis. Even if this reporting could occasionally include data related to DFPS, specific, regular and standardised regulatory reporting related to the provision of DFPS does not seem widespread. Out of 24 respondents, 17 said they have general periodical data-reporting requirements (not only for DFPS) that include some data related to the provision of DFPS, while only two respondents have specifically elaborated this kind of reporting.

Survey respondents highlighted the need to adapt the scope of the reports in order to collect information on both products and channels. They also would like to see new mandatory reports on specific information related to DFPS and their risks, such as security and operational incidents, where these are not yet available.

A few authorities have the capacity to collect other types of information from financial services providers that can be used in supervising DFPS, such as changes to product terms and conditions. This provides valuable input in identifying market trends and helping to ensure DFPS- related consumer protection.

SupTech has been identified by some authorities as a potential tool to enable more real-time reporting and provide access to greater volumes of data. Supervisors can use advanced data analytics to supervise entities and monitor risk in the market. This aspect is mentioned in 3.6 below. Some authorities feed all input obtained via the above-mentioned tools into structured databases. These databases are then used to monitor DFPS developments, emerging risks and their implications.

Some authorities that are introducing rules for specific DFPS, are using that opportunity to introduce comprehensive supervisory reporting.

Indonesia OJK: off-site surveillance of FinTech P2P lending providers

P2P providers must submit periodic (monthly and annual) reports. They must include:

- performance
- financial and operational overview
- consumers' and business partners' testimonials
- achievement and certification
- management report
- company profile
- reviews of business support units (IT, human resources)
- analysis and management review (financial, macroeconomic, industry, business, marketing, business prospect and upcoming strategy)
- corporate governance (risk management, internal control, ethics code, transparency, consumer complaint handling and mechanism)
- transaction numbers
- database (lender and borrower demography)

Indonesia OJK conducts digital off-site evaluation by analysing the periodic reports from P2P providers. To enhance this, OJK is currently developing a supervisory application/system connected directly to FinTech providers' systems, to gather company data and information on a daily basis.

Other authorities follow a different approach to data reporting, for example through reception of information with a special focus on new products:

Central Bank of Ireland: Conduct of business returns (COBRs)

The conduct of business returns (COBRs) request details of changes to product offerings, including changes to terms and conditions of products, and retail product developments over the coming six months. The COBRs provide information on new products offered in the period, products withdrawn in the period, changes to terms and conditions of products in the period, and retail product development.

The information about changes in product offerings is mainly qualitative and can provide insight into market trends. The central bank amalgamated all COBRs in an integrated, searchable platform. Changes in product offerings can be used to review historical

developments, or developments within certain sectors or product areas. This tool is not specific to DFPS, although it has been used to review:

- the introduction of contactless functionality for off-sale cards
- inclusion of contactless functionality on new and reissued debit cards
- the mobile P2P service
- the update to existing mobile banking apps with a new design and the addition of new features

Other initiatives related to reporting of new products

Portugal

On January 17, 2018, **Banco de Portugal** issued a circular-letter to credit institutions and financial companies that provide clients with access to digital channels to initiate and conclude the process of contracting consumer credit products. These firms shall provide Banco de Portugal with information on the characteristics of the product, the details of the contracting process and the security mechanisms implemented. This information shall be provided by completing a questionnaire that shall be sent with at least 10 business days prior to the date on which the product is to be marketed. In addition to the questionnaire, the pre-contractual information documents relating to the product concerned, as well as the respective product data sheet, shall also be sent.

Peru

Peru's Superintendency of Banking, Insurance and Private Pension Funds Administrator (SBS) issued Resolution 272-2017 and Circular G-165-2012. These require that entities assess the risks and market conduct issues associated with new products and important changes in business, operational or computer environments. In this sense, entities elaborate a report containing i) information about the new product or important change, ii) description of the identified risks by category, and iii) results of the risks' assessment and the treatment measures that were defined or implemented. This report must be approved by the entity's risk committee and provided to the SBS immediately after the new product is launched, or prior the execution of important changes.

Japan

Japan Financial Services Agency (FSA) requires that each crypto-asset broker-dealer submit an annual business report in respect of its crypto-asset exchange services. It also requires a periodic report on the amount or quantity of users' money and crypto-assets managed by the crypto-asset broker-dealers. In the registration procedure, FSA checks the appropriateness of the internal structure and the governance system of the entities, with special attention to system security, measures against cyber-attack; AML/CFT; segregation of assets of users from those of crypto-asset exchanges (both for crypto-asset and deposited cash) and proper and timely explanation of risks to users.

Canada's FCAC is planning to adopt a business intelligence strategy and enhance business intelligence tools to support decision-making, information-sharing and research. The strategy will help the Agency identify and collect data it can trust, and use it to make evidence-based decisions in carrying out its mandate.

Takeaways

Data reporting	Specific data reporting for DFPS is a very important tool that can provide an overview of the digital products and services that are being launched in the market and on their respective characteristics. Security incident reporting should be encouraged to mitigate security risks.

3.3. On-site inspections

On-site inspections are a fundamental tool in ensuring a sound supervisory framework. In principle, it is only through on-site supervision that authorities can collect certain types of information and perform certain checks needed to understand how systems and networks are operating. Through on-site supervision, authorities can check data reliability and discuss and assess the assumptions, methods, and systems used in DFPS. In addition, the on-site component facilitates continuous contact with supervised entities.

Some respondents believe there is no need to adapt on-site inspections to digital products and services, while others have pointed out how traditional supervisory tools may be adapted to the on-site supervision of DFPS.

First, some authorities believe there is a need to develop mechanisms that allow access to credit institutions' technological platforms in order to keep up with the processes and phases in DFPS distribution.

Second, many respondents underline the need to obtain technical expertise and recruit adequate inspection teams to design new technical tools in order to run validations that may check the legal compliance of the processes of distribution through digital channels and, at the same time, develop tools to assess risks related to DFPS and their controls.

According to the survey responses, several jurisdictions have not yet performed specific on-site inspections of DFPS. Other authorities are planning to do so, while others occasionally introduce some aspects related to the digital channels in their "traditional" inspections.

Generally speaking, respondents that have performed any form of on-site inspection refer to work undertaken in relation to IT systems, cybersecurity, governance and capabilities of institutions, including information security controls, product and services developments applied to DFPS, and especially focused on firms more active in the commercialisation of DFPS. Moreover, thematic or specific on-site inspections have been performed in relation to cloud computing, robo-advisors, pre-contractual information and P2P lending banking agents.

In most cases, authorities are currently designing their specific plans for developing on-site supervision of DFPS. The most recurrent type of checks that supervisors are planning are intended to ensure that the relationship of customers with financial providers fulfils all transparency rules at all stages of that relationship (advertising, pre-contractual information, contractual information, life of the contract). These checks can be developed in the course of a traditional on-site inspection with intensive participation by IT staff who analyse the interfaces and their scripts.

Respondents are exploring other innovative and effective tools. For this purpose, supervisors may have to obtain from supervised entities the authorizations to simulate, in a real environment (at least in testing mode), a client's full interaction with the digital interface throughout the contracting process. This option may even be used off-site if the appropriate permissions from the entities are obtained.

With the possibility of running such a tool, supervisors could review the whole cycle of the relationship between provider and customer, according to the rules in each jurisdiction, and check aspects such as:

- whether general information and pre-contractual information fulfil the rules
- the practical aspects of the digital interface, to ensure they do not jeopardise the measures established in each jurisdiction's rules to protect customers
- whether the form of accepting the terms and conditions (the way in which the contract is finally signed) is technically adequate

Mystery shopping has obvious limitations in the digital world. For example, when initiating use of online banking apps, before getting to the essence of the contracting process, apps request some types of user identification (account number, telephone number, etc.) that make it difficult for authorities to play a role similar to that of a mystery shopper. In fact, the supervisors need to play the role of a "virtual shopper" that is allowed to operate the apps.

Hence, the provision of financial services online may give rise to a review of the value of mystery shopping as a supervisory tool, possibly leading to its adaptation, particularly through the use of technological and innovative means.

To adapt traditional mystery shopping to DFPS, authorities would have to gain remote access to the institution's system in order to simulate, for instance, the process for contracting a product; the system accessed by supervisor would have to be identical to the entities' production system.

It would be ideal if authorities had permanent access, without previous warning, to an institution's app, to verify app compliance with legal requirements and monitor changes introduced over time. Additionally, it would be possible to test several scenarios, profiles, use cases, inspired by real situations (based on a complaint submitted by a client, for example).

Only a few of respondents referred to experience in on-site inspections in relation to DFPS.

Central Bank of Brazil: P2P lending banking agents

During 2016, the Central Bank of Brazil inspected the performance of some DFPS acting as P2P lending banking agents. In this review, the central bank identified issues related to transparency (especially with regard to information available on the website) and compliance with current regulation.

According to the Brazilian rules (Resolution 3.954 of February 24, 2011), the banking agent acts on behalf of, and under the guidelines of the contracting institution. That institution assumes full responsibility for the service provided to clients and users through the contractor. The contractor is responsible for ensuring the integrity, reliability, safety, and the confidentiality of transactions it carries out, as well as compliance with the legislation and regulations relating to such transactions. This resolution also establishes that the agent must disclose to the public its condition as a provider of the contracting institution, identified by the name with which it is known in the market, with a description of the products and services offered and telephone numbers of customer service and of the contracting institution.

As a result, the financial institutions demanded from their banking agents the regularization of breaches and weakness detected. In some cases, financial institutions have chosen to disqualify banking agents. The main lesson learned was that regulation needed to be improved to better address DFPS. As a consequence, the Central Bank of Brazil studied the regulation of peer-to-peer (P2P) lending. On April 26, 2018, the Brazilian National Monetary Council (CMN) published Resolution 4.656, which establishes requirements and procedures for lending and financing transactions among individuals through electronic platforms provided by FinTechs. The Resolution attributed to P2P lending companies the status of financial institutions in their own right, as an alternative to acting as P2P lending banking agents, which implied relying on incumbent financial institutions to operate in the Brazilian domestic market.

The Central Bank of Ireland undertakes pre-authorisation inspections of applicants undertaking DFPS activities. This is to i) obtain a walkthrough of the service proposed via the firm's systems in order to understand better aspects of activities and obtain comfort that systems do what they are designed to do and that the necessary controls are in place at each stage in the process; and ii) meet individuals who will be involved in the firm's day-to-day activities and obtain comfort regarding their competence and understanding of applicable requirements.

The Netherlands AFM intends to assess IT governance and the maturity of IT risk management of DFPS by using self-assessments in combination with on-site visits. These self-assessments will combine (generic) IT governance (based on generally accepted frameworks such as COBIT) with thematic deep dives on specific risks (e.g. outsourcing, cloud computing and machine learning/AI).

Given the importance of online payments in the digital age, Chile has emphasized specific reviews in the areas of payments. Chilean authorities indicated that reviews are underway on the use of soft tokens by financial institutions to authorise electronic transfers of funds online, and the identity theft and the risks of criminals intercepting authorisation codes in the network in order to change parameters, such as recipients and transaction amounts.

Other authorities are exploring facilities that may allow supervisors to reproduce the digital interface for customers.

Central Bank of Brazil:
Monitoring screens used in digital channels and digital contracting processes

The Central Bank of Brazil verifies product and service compliance with the rules in force, especially those related to transparency and the offerings' suitability to the consumer. Only the main products of a supervised entity are verified. In recent years, the central bank has dealt with new products in all areas (deposit account, payments, investments and credit, among others) that use digital channels. When there are signs of problems with a product, the central bank may conduct an on-site inspection.

One of the ways the central bank checks compliance is by verifying the screens and steps shown to customers in offering and contracting the product/service. The central bank does not have access to the screens used to contract financial products. They require supervised entities to present them, whenever it is deemed necessary.

The experience of Banco de Portugal

Before a new digital product is launched in the market, the institutions must report it to Banco de Portugal which validates the contracting process thought the digital channels, among other aspects. To guarantee not only the compliance of the products and the information duties, Banco de Portugal inspect all the screens, the applicable legal information requirements and the security and authentication mechanisms used to identify the client.

If Banco de Portugal notices any problems with the product or contracting process, conduct supervision teams use enforcement powers or moral suasion (recommendations) so the financial institutions make the required amendments in order to comply with the applicable legislation in force or applicable best practices.

Takeaways

On-site inspections and off-site remote access	To gain insight into the contracting steps customers follow in transactions conducted on the different screens shown on digital devices, supervisors need the right technical tools to access such screens and steps in real time. This is to check whether the screen content and steps respect legal requirements in terms of transparency (pre-contractual and contractual information). These checks could be done with the participation of IT staff employed by authorities. They may review the apps and any other interfaces, including their scripts. IT staff may do so through on-site inspections or off-site remote access to the digital interfaces of the entities in live mode. As technology evolves, new matters become subject to inspection, such as IT systems, big data, scoring models, robot advising, etc.

3.4. Other supervisory tools

3.4.1. Cooperation

Cooperation among national and international financial services regulatory and supervisory authorities in the field of DFPS is a key factor in improving financial consumer protection. In addition, they need to cooperate with other authorities, beyond market conduct supervisors, that may have a relevant role in digital services. The table below shows the degree of cooperation between conduct authorities and other authorities, as indicated by the 24 survey respondents.

Table 10 Cooperation with other authorities

Cooperation with	Number of authorities
Relevant regulators in their jurisdiction	18
Anti-money laundering authorities	18
Other supervisors outside their jurisdiction	16
Other financial supervisors in their jurisdiction	13
Data-protection authorities	13
Competition authorities	13
Other authorities in their jurisdiction	12
Telecommunications regulators	6

As highlighted in the table above, the majority of respondents with relevant regulators in their own jurisdiction on policy developments and with anti-money laundering authorities. Nevertheless, there are other important forms of cooperation: with other national and foreign supervisors, with data-protection authorities and with competition authorities. The authorities that are leading supervisory breakthroughs show a very proactive approach in signing cooperation agreements with overseas regulators and supervisors.

One-quarter of respondents explained that, although there are some formal agreements or memoranda of understanding (MoUs) among authorities, there is also informal collaboration. In some jurisdictions, the main form of collaboration is information exchange.

Some countries have established formal groups and joint committees to address DFPS supervision issues. In one case, the central bank and the markets authority are collaborating in an innovation hub in that jurisdiction. In another country, the central bank has established an internal group regarding cybersecurity, collaborating with other authorities at the national level. In other jurisdictions, there are fora and working groups concerning FinTech.

In February 2018 the Basel Committee on Banking Supervision published a report, *Sound Practices on the Implications of FinTech Developments for Banks and Bank Supervisors*. It highlights the usefulness of the communication and coordination between bank supervisors and other authorities in charge of, for example, data protection, fair competition and national security.

Canada's federal government has created the Financial Institutions Supervisory Committee (FISC). This important committee meets regularly to share information, coordinate actions, and advise the federal government on financial system issues, including those related to DFPS. The committee includes representatives from the following federal government entities: the Department of Finance, Financial Consumer Agency of Canada, Office of the Superintendent of Financial Institutions, and the Canada Deposit Insurance Corporation.

Some jurisdictions founded on a sectoral model have set up committees jointly with other authorities with the objective of sharing information and ensuring activities are coordinated. This is the case of the Banco de España collaborating with the Ministry of Economy and Business through its General Secretary of the Treasury and Financial Policy, the National Securities Market Commission (CNMV) and the General Directorate for Insurance and Pension (DGSyFP). Together they analyse the impact of innovation and digitalisation on the financial sector. That is also the case of ACPR in France, which cooperates with the French Autorité des Marchés Financiers; their coordination extends to DFPS supervision matters.

With regard to international cooperation, the UK FCA has signed nine collaboration agreements with overseas regulators in the framework of its innovation hub: Australia (ASIC), Singapore (MAS), Korea (FSC), China (PBOC), Hong Kong (HKMA, and HKSFC), Canada (OSC), Japan (FSA), and the USA (CFTC).

The Australian Securities and Investments Commission (ASIC) Innovation Hub has signed a number of international FinTech cooperation agreements that aim to assist innovative businesses in Australia make ventures into international markets. These agreements will help break down barriers to entry by enabling ASIC to refer FinTech start-up businesses to international regulators to efficiently establish initial discussions and receive informal assistance on the regulatory environment they may face. These arrangements include: referral and information sharing agreements with UAE (FSRA, DFSA), Canada (OSC, CSA), United Kingdom (FCA), Singapore (MAS), Hong Kong (HKSFC), Malaysia (SC) and

Switzerland (FINMA); information-sharing agreements with China (CSRC), Indonesia (OJK), Kenya (CMA) and Exchange of letters with Japan (FSA)[6].

Cooperation in the field of digital innovation is not confined to financial authorities. In some cases the respondent authorities collaborate with:

- telecommunications regulators (cooperation between the Bank of Mauritius and the Information and Communication Technologies Authority regarding mobile banking)
- data-protection authorities (in Luxembourg, the CSSF cooperates with the Commission nationale pour la protection des données in FinTech working groups)
- other relevant authorities in the technology sector (Banco de Portugal is exchanging information on security incidents with the National Cybersecurity Centre and has created its Computer Security Incident Response Team (CSIRT) with regard to cybersecurity; BaFin (Germany) closely cooperates with the Federal Office for Information Security (BSI)).
- FinPay (Finance Canada Payments Consultative Committee) is a forum of public and private sector representatives to discuss industry-level developments in the Canadian payments system. FinPay's mandate is to: advise the federal Department of Finance on developments related to public policy aspects of payments issues (e.g. competition, innovation, safety, user needs or consumer protection); discuss approaches for dealing with emerging and ongoing challenges/opportunities in the payments system; and inform government policy-making about the Canadian payments system.

Takeaways

Cooperation	There are many reasons for supervisors to engage and cooperate actively and effectively with other authorities in charge of supervision in relation to all DFPS matters. Doing so may help supervisors to gain a broad view of DFPS implications (different sectors, cross-border, technological, anti-money-laundering, data protection, etc.). It may also help to coordinate efforts and avoid overlaps, in order to understand DFPS development and identify potential risks.

3.4.2. Issuing guidelines, best practices, consumer protection principles

Some authorities indicate they have issued guidelines or recommendations that affect DFPS. In some cases guidelines have been issued in relation to digital issues specifically, while in other cases certain existing guidelines related to traditional products have been amended to include the specificities of provision of these products and services by digital means. One respondent points out that these kind of guidelines should be more principle-based instead of rule-based.

6 Authorities mentioned in this section that are not included in the annex listing survey respondent authorities are: MAS: Monetary Authority of Singapore; Korea FSC: Financial Services Commission; PBOC: People's Bank of China; HKMA: Hong Kong Monetary Authority, HKSFC: Hong Kong Securities and Futures Commission; OSC: Ontario Securities Commission; CFTC (Commodity Futures Trading Commission); FSRA: Financial Services Regulatory Authority; DFSA: Dubai Financial Services Authority; CSA: Canadian Securities Administrators; SC: Securities Commission; FINMA: Swiss Financial Market Supervisory Authority; CRSC: China Securities and Regulatory Commission and CMA: Capital Markets Authority of Kenya

Some countries have already issued guidelines specifically focused on DFPS especially related to IT, outsourcing and cybersecurity issues, and in relation to specific matters like digital advice, P2P lending, distributed ledger technology (DLT) and block chain or VC.

Survey respondents mentioned several examples of guidelines.

- The Central Bank of Ireland has issued a Cross-Industry Guidance in respect of IT and cybersecurity risks.
- Indonesia OJK has implemented consumer protection principles for both the borrower and the lender using P2P lending services.
- Japan FSA has set the supervisory guidelines for crypto-asset broker-dealers.
- ASIC has issued guidance on providing digital product advice to retail investors, Information Sheet 213 on marketplace lending (P2P lending) products, Information Sheet 219 evaluating DLT, and recently two regulatory guides for intermediaries seeking to provide crowd-sourced funding (CSF) services and for companies seeking to raise funds on a platform of a CSF intermediary.
- The Bank of Mauritius has issued a Guideline on Mobile Banking and Mobile Payment Systems, a Guideline on Internet Banking, a Guideline on IT risk Management and a Guideline on Control of Advertisement.
- BaFin (Germany) published a Circular (Bankaufsichtliche Anforderungen an die IT (BAIT)) specifying the minimum requirements for risk management concerning IT security in the banking sector.

France ACPR: recommendations for social media use in financial advertising

In 2016, ACPR in France issued recommendations for the use of social media in financial advertising by entities under its supervision. The recommendations covered: i) the identification of the issuer of advertising (natural and legal persons), ii) the way of presenting information (clear and honest, clear indication which allows the identification of the advertising, mention of additional information) and iii) the way of storing information and control procedures (to define rules and control procedures and the implementation of an archiving policy).

Takeaways

Soft regulation	The issuance of supplementary regulatory materials such as guidelines, position notes or warnings may be an effective supervisory tool to discipline certain DFPS segments. These tools may be a valid alternative to amending the global regulatory framework, which may require a long legislative process.

3.4.3. Licensing and authorisation regimes

The change in business models and the provision of products and services by financial providers through digital means may require an adaptation of licensing and authorisation requirements currently in place in some jurisdictions.

Adaptations in the licensing and authorisation regimes should be introduced following regulatory changes. Most likely these changes will follow the introduction of certain types of providers in the scope of regulated entities in a jurisdiction. In any case, and regardless of

the eventual introduction in the scope of regulation of new entities, the general licensing rules might be adapted to reflect the risks posed by DFPS, increasing the focus on understanding the business models and the nature of the new DFPS and on ensuring the adequacy of the governance arrangements in place.

Regulatory sandboxes can also play a key role in licensing processes by providing jurisdictions with a way to observe DFPS-provider operations prior approving their licence. Innovation hubs and regulatory sandboxes are discussed further in chapter 4.

One case of specific regulation that introduces a new framework for licensing new types of entities is that of Japan FSA's licensing of crypto-asset broker-dealers. FSA introduced a registration framework for exchange-service providers of crypto-assets for legal tender, obliged such providers to conduct user-identity verification, and introduced certain provisions to ensure user protection, such as providing information to users as of April 2017.

Another initiative observed in Europe consists of revised rules for payment services within the European Union. These seek, among other objectives, to enable existing and new service providers, such as account information service providers[7] and payment initiation service providers[8], to offer their services in a clear and harmonised regulatory framework. European Directive PSD2 foresees specific registration/authorisation regimes for these providers.

The Central Bank of Brazil has also started promoting adaptations in the licensing and authorisation regimes. The enactment of Resolution 4,656 on April 26, 2018 attributed P2P lending companies the status of financial institutions, enabling them to operate in the Brazilian market without relying on incumbent financial institutions. The Central Bank of Brazil also issued Circular 3,898 in May 17th, 2018, which determines the procedural rules for establishing P2P lending companies. By the end of 2020, the Central Bank of Brazil intends to introduce adaptations to the licensing and authorisation regimes following regulatory changes impacting business models and the provision of DFPS.

Takeaways

Licensing and authorisation	Regardless of the introduction in the scope of regulation of new entities, the general rules on licensing might be adapted to reflect DFPS risks. This would mean increasing the supervisor's focus on understanding an entity's business model and the nature of new DFPS; and ensuring the adequacy of the governance arrangements in place with regard to IT systems used to provide DFPS.

3.4.4. Financial education

Financial education programs related to DFPS can increase consumer awareness about the risks related to these products and may contribute to the global goal of conduct supervisors mitigating risks to consumers. Of 24 respondents, 15 said financial education initiatives in their jurisdiction include raising consumer awareness of the risks associated with DFPS.

7 Account information service providers allow a payment service user to have an overview of their payment accounts, held with either another payment service provider or with more than one payment service provider, at any time.
8 Payment initiation service providers allow consumers to initiate a payment order with respect to a payment account held at another payment service provider.

In some countries, the supervisory authority does not have a mandate for financial education; instead, it is undertaken by the government or in co-operation with other authorities. All the same, the supervisory authorities issue warnings and notices to consumers.

Program objectives are not only to explain the risks associated with certain products and to promote precautionary attitudes by digital products and services users, and promote confidence in financial providers.

Moreover, many respondents indicate training sessions and other campaigns are being launched on specific matters such as security issues, crowdfunding, VC, alternative payment methods, etc. One respondent mentioned the use of digital channels, such as social media, to encourage consumer financial literacy and to ensure education reaches a broad public.

Australian Securities and Investments Commission: developing the MoneySmart project in the context of financial education

The MoneySmart website is one of the key initiatives in the National Financial Literacy Strategy that provides a practical framework for encouraging the improvement of financial literacy for Australians. The MoneySmart website offers consumers free, independent guidance on a number of topics. In this regard, MoneySmart has included specific information about some DFPS such as crowdfunding, VC, P2P, remittance, cardless banking and contactless cards. In general, consumers can find webpages on these topics that contain a definition of DFPS, its functioning, risks and practical information about its use.

Banco de Portugal: strategic plan for 2017-2020 establishes digital financial literacy goals

Banco de Portugal's digital financial literacy strategy addresses young people and adults, security being the most important issue. This strategy is implemented through training sessions and seminars at schools, leaflets, booklets and other materials for young people and their teachers and awareness campaigns on banks' customer-facing websites.

Additionally, Banco de Portugal has developed relevant content for the bank customer website on the major security risks related to online and mobile payment services. In March 2016, Banco de Portugal launched on its website a campaign about online safety and fraud prevention, to raise consumer awareness on security issues. Banco de Portugal is also developing training sessions, mainly at schools, regarding advantages, risks and security measures related to DFPS.

Canada FCAC: educational web content related to DFPS

In the context of financial education, FCAC provides information about digital financial services, including information to raise awareness of the potential risks. This content includes information on the following topics:

- online banking: how to protect consumers from unauthorised transactions when banking online; consumers' responsibilities when banking online; how to protect personal information online
- mobile payments: the risks of using a mobile device to make a payment; how consumers are protected against unauthorised mobile payments; how to make a

complaint about a mobile payment; tips for consumers on protecting their mobile device
- mobile wallets: tips for using mobile wallets securely; consumers' rights related to the Code of Conduct for the Credit and Debit Card Industry in Canada
- digital currencies (or cryptocurrencies): risks and tips
- remittances: information related to sending money to someone in another country

Regarding non-transactional digital financial services, FCAC has issued a consumer alert about the potential risks of using financial services aggregators.

In Indonesia, the OJK requires P2P lenders to undertake education activities and to submit a report to the OJK detailing the education plan and the effectiveness of the activity performed.

Other respondents link financial education with financial inclusion, assuming that without education, the availability of digital channels and devices may not be enough to guarantee inclusion.

Peru's SBS: financial education and financial inclusion

Peru's SBS understands that digital financial services are one of the main alternatives to traditional financial services in reaching a large number of the unbanked population, but its implementation comes with big challenges on both the supply and demand sides. The Peruvian government has established financial inclusion as a priority under its social-inclusion goals. The financial literacy working group under the National Strategy for Financial Inclusion, which is led by the Ministry of Education and the SBS, designed the National Plan of Financial Education. It seeks to improve financial competencies and capacities of all segments of the population for proper decision making and better control of their own finances. One main achievement of this working group is the enhancement of the Peruvian national curriculum for schools, approved in 2017, which incorporates financial literacy as one of its 29 competencies required in students aged 6 to 17 years. Moreover, the curriculum integrated a cross-cutting approach with other competencies, such as the information and communications technology (ICT) competency, generating capacities in the students for exercising their consumer rights in digital financial contexts.

Takeaways

Financial education	For most authorities with responsibilities in financial education, there is a clear link between the promotion of the level of financial and digital education of customers, and the impact of efforts to mitigate risks associated with DFPS. Even where financial education is not viewed as a supervisory tool, it may boost the effectiveness of other supervisory tools.

3.4.5. Moral suasion

Although there is no formal definition of supervisors' "moral suasion", the majority of supervised institutions tend to adhere to supervisors' opinions/recommendations, including those transmitted in meetings with an institution's senior management, even when these recommendations are not legally binding. Given that moral suasion invariably involves a discussion with the senior management of a regulated financial provider, the approaches are not expected to vary considerably between a DFPS issue and a traditional one.

South African Reserve Bank (SARB): moral suasion in DFPS provision

In the SARB's early years of addressing cryptocurrencies, banks were informally steered away from engaging in activities deemed too risky, rather than using formal communication, such as letters. Such moral suasion is a useful tool in stopping behaviour that may be raising concerns. The SARB working group, through the National Payment System Department, also uses position papers as a tool of moral suasion. For example, this working group published a position paper on VC in 2014.

3.4.6. Behavioural economics

Although few respondents use behavioural economics to guide their policy actions, some acknowledge the relevance of this tool in generating effective regulations. Behavioural insights can be used to design policies and test the effectiveness of these policies in practice by running randomised controlled trials, noting that consumer behaviour may be different when obtaining financial products through digital channels rather than traditional channels.

Digital environments are relatively new, and human behaviour in such environments has particular aspects that need further analysis. It is obvious that the process of contracting financial products through digital channels implies some bias that may incorporate additional risks. The application of behavioural intelligence to DFPS supervision has huge potential.

Addressing consumer behaviour in digital interfaces is particularly challenging. In this context, Banco de Portugal is considering a rule establishing information-disclosure duties would be fulfilled only if the interface forces the customer to scroll-down the documents completely.

The Australian Securities and Investments Commission (ASIC) established a dedicated behavioural economics team in 2014. ASIC's Behavioural Unit consists of behavioural economics, consumer research and consumer policy functions. ASIC publications reveal that small details matter in a digital environment (e.g. screen size, timing, order, channel, presentation, etc.) and can influence how much engagement and attention customers are able to give in any given context.

Canada's financial literacy strategy incorporates behavioural economics research into initiatives to improve the financial well-being of Canadians, and to enrich understanding of how technology can help consumers with their choices. FCAC builds on research to learn how mobile applications and other technologies can promote and influence behavioural changes.

Takeaways

Behavioural economics	DFPS introduce additional complexity to the consumers' decision-making process. The advantages of DFPS to customers–ease and speed of transactions–simultaneously create incentives for consumers to enter into transactions without properly analysing their financial implications. For these reasons, regulators and supervisors should consider behavioural insights as they conduct their activities.

3.5. Digital expertise, IT reviews and technological outsourcing

3.5.1. Digital expertise

Supervision of DFPS provision requires IT expertise to match the demands of the DFPS marketplace. For this reason, 13 out of 24 respondent authorities have already integrated or foresee the need to integrate IT experts in their conduct supervision teams. Nevertheless, IT staff already integrated in conduct supervision teams are often specialised in traditional inspections based on the analysis of databases (checking entities' files with information related to traditional products), but not on digital aspects. The challenge for conduct supervision authorities is not only quantitative, in creating teams with adequate IT resources, but also qualitative in incorporating staff with the adequate digital expertise.

Responses from the authorities differ significantly. Eight authorities said IT experts are not involved in supervision of consumer risks associated with DFPS. Authorities that also have prudential supervision mandate frequently refer to the existence of specialised IT groups that undertake prudential supervision, not conduct supervision. These IT experts are mainly dedicated to the analysis of IT risks (operational risk) from a prudential perspective that focuses on risks for the entity itself. Although this supervisory activity is not explicitly focused on identifying risks for customers, it is clear there are some synergies.

Takeaways

The technological challenge associated with DFPS requires a huge effort from supervisors to incorporate in their structures the knowledge that may allow them to understand the functioning and risks of digital channels.

Digital expertise	To face the digital challenge full-on, it may be advisable for supervisors to: • train and keep up to date existing staff so they develop and maintain sufficient technical knowledge to control complex financial technology adequately • increase the number of IT experts available for conduct supervision, and ensure they have specific skills relevant to supervising DFPS • seek that the IT experts working in conduct supervision follow an approach that, building on previous IT risk already developed by many authorities that is often focused on IT risks for entities, escalate to an approach that analyses the risks for consumers and very specifically scrutinise the contracting process by digital means.

3.5.2. IT reviews

The recruitment of IT experts can help in conducting on-site inspections to assess the adequacy of an institution's IT systems, legacy and Internet-based systems architecture, IT governance, information/cyber security, IT internal audit and IT compliance and contracts outsourcing work to other providers. There are different ways to approach the technological risks. Authorities such as the Central Bank of Ireland, Germany BaFin, and Autorité des

marchés financiers du Québec (AMF) have undertaken work in relation to the quality of IT systems in regulated firms or cybersecurity.

The Central Bank of Ireland has set up a cross-divisional group (IT and Cyber Risk Strategy Group) to look at common IT and cyber risks across entities supervised by the central bank, with stakeholders from various divisions such as prudential supervision, consumer protection, financial stability, etc. The group focuses primarily on cyber risk and published cross industry guidance in respect of IT and cyber-security risks. Other authorities refer to the existence of specific structures focused on IT, such as the IT and FinTech Strategy Department of Korea Financial Supervisory Service (FSS) or the Department of Operational and Technological Risk in Chile Superintendency of Banks and Financial Institutions (SBIF).

Autorité des marchés financiers du Québec (AMF) carries out inspections of IT general controls (e.g., information, security controls, product and services development) that apply directly to DFPS and inspections of specific products or activities (e.g., online trading, online banking). These IT controls cover regular topics (e.g. business continuity planning, information (cyber) security, outsourcing, development, etc.). These programs are developed using recognised international standards (e.g. ISO, NIST, ISACA/COBIT). The data analysed throughout these inspections are mainly qualitative in nature. It comes from reports issued by the different lines of defence of the organisation (IT operations, risk management, compliance, internal and external audits, board and committees).

The same authority conducted a survey in 2015-2016 among the top 80 financial institutions operating in the province of Québec to assess their cyber-security posture. Based on the best practices recommended by the ISO, NIST and ISACA/COBIT frameworks, financial institutions were asked to evaluate the maturity level of their practices across their organisations. AMF considers that cyber threats must form an integral part of the risks managed by institutions and that integrated risk management must be underpinned by a solid governance structure that assigns accountability to senior management and the board of directors.

3.5.3. Technological outsourcing

The outsourcing of certain processes or activities is particularly relevant for DFPS provision, given that these kinds of products and services are usually offered online and the operators of the respective online platforms might not be located in the jurisdiction where the products and services are marketed. It is commonly understood that responsibility for outsourced activities should remain with the financial entity.

Almost half the respondents indicate that their supervisory authority reviews agreements signed between supervised financial entities and external technology service providers in general, and also in relation to DFPS. Many authorities are reviewing agreements through a prudential approach, that is, to anticipate risks for the financial entities. These reviews typically imply checking compliance against applicable rules, service-level agreements, and business continuity and information disclosure clauses. In some cases, the examination covers all significant outsourcing activities while in others, authorities' checks are performed on a sample basis.

Contract examination is performed from a legal perspective rather than from a technical view of the service outsourced. These reviews are done during on-site inspections and in licensing processes, and they are carried out from a prudential rather than market conduct view.

Luxembourg's Financial Sector Surveillance Commission (CSSF) analyses all contracts signed between supervised financial entities and external technology service providers in relation to DFPS. It does so during the authorisation procedure and during the supervision of DFPS providers. This review is carried out to verify whether the legal outsourcing requirements are respected. The scope of this review is financial stability and consumer protection.

The German banking act provides for the possibility of checking outsourcing arrangements in the course of general risk-management inspections. BaFin reviews any outsourcing agreements to ensure services are being provided in a proper manner and in compliance with supervisory law.

In a similar way, the Central Bank of Brazil published Resolution 4,658 on April 26, 2018. In the case of foreign outsourcing companies, the resolution requires financial institutions to certify the existence of a memorandum of understanding (MoU) between the central bank and the supervisory authorities of the countries where the services are provided. If there is no MoU, the institution must obtain prior authorization from the Brazilian central bank to contract or retain the services, provided that access to data and information abroad by the contractor and by central bank staff is neither impeded nor restricted.

Takeaways

DFPS cannot be addressed without also addressing the outsourced contracts on which they frequently depend. Supervisors cannot ignore the potential impact of such contracts on the risks assumed by the financial provider and consumers.

Technology outsourcing	In accordance with their specific regulatory set up, each supervisor may have to review, outsourced activities, including aspects like the complaint systems related to outsource services, the chain of outsourced providers and the concentration in a few of them.

3.6. SupTech

New technologies and digital developments not only imply risks that must be mitigated by supervisors, but also opportunities to develop technology-intensive tools that ease their work. Supervisory technology (SupTech) has been defined as the application and use of technology by supervisors to carry out their supervisory and surveillance work more effectively and efficiently. Through the use of these tools, the challenges posed to supervisors by the evolution of technology and the digitalisation of the banking sector may be mitigated.

About one-third of respondents confirmed the use of SupTech solutions, while some other are exploring its application. All supervisors use some sorts of supervisory tools based on technology and it is a question of nuance whether supervisors consider these technical solutions to be SupTech tools. The respondents applying SupTech have referred to the use of artificial intelligence (AI), DLT, cloud computing, etc. These tools are applied in a two-fold approach: first, to detect new business models and second, by using specific innovative tools for in supervisory checks.

In parallel, complaints handling services (sometimes operated by supervisors) are benefiting from the possibilities offered by the new technologies. Various respondents indicate speed and flexibility are very important in the complaints handling process. In this sense, handling claims through digital channels is generally used, while other tools related to the use of social networking are being explored, ensuring that it is effective and secure in the delivery of information.

A few respondents highlighted their use of the following SupTech approaches:

- monitoring social media platforms, blogs and online content to identify and assess innovative products
- real-time surveillance systems to detect market abuse
- big data information analysis to prohibit clandestine practices by intermediaries
- cognitive tools to analyse service-provider web pages
- machine-learning applications to assess document sets to identify evidences in inspections
- market analytic tools to help identify connections between entities

France's ACPR: interest in SupTech tools

ACPR's interest in SupTech solutions relies on the Bank of France's new innovation lab, launched in June 2017. Le Lab Banque de France is an open innovation laboratory whose goal is to bring new practices and technologies into the bank's activities and identify, explore and test new technologies for i) new working patterns and methods such as design thinking, visual management and chatbots, ii) advanced data analysis such as AI, data science, cognitive computing and iii) innovative technological opportunities such as block chain, "internet of things" (IoT) and virtual reality.

Takeaways

SupTech	Technological development can enhance supervision through the incorporation of cutting-edge technologies into supervisors' procedures.

3.7. RegTech

RegTech tools are innovative solutions implemented by financial service providers to meet regulatory requirements, address regulatory changes and enhance automatic risk management more effectively and efficiently. From this perspective, it is obvious that supervisors are interested in ensuring the accuracy of the tools used. In addition, RegTech solutions may interfere the way in which supervisors receive mandatory information from financial entities. For these reasons, supervisors should follow closely the RegTech developments and even promote or steer them.

Various authorities have taken action to analyse these tools. Some respondent authorities mention that financial providers in their jurisdiction are using RegTech to:

- detect new regulation that might affect the financial provider
- optimise regulatory reporting
- systematise analysis to ensure compliance with different sets of regulation, such as "know your customer" (KYC) or AML (fraud detection and controls automation)

- improve efficiencies in interpreting and implementing regulation (such as robo-assistants and semantic technologies)
- help firms to leverage their data assets (such as real- and near-time analytics and compliance monitoring)
- provide new ways of interacting with clients (chatbots) or to provide advice/recommendations (robo-advisor)

In the example of AML checks on payment transactions, the tool applies different big-data analysis that continuously scans the customer's incoming/outgoing payment transactions against pre-defined criteria (related to unusual amounts for that payer, an unusual payee, transactions to countries listed as being at higher AML risk, etc). If the criteria are recognised (i.e. "hits" in a payment transaction), the payment transaction can be blocked automatically.

These new tools may have consumer protection implication, so various authorities are monitoring these technologies and may recruit expert staff to supervise them. For now, regulators are mainly interested in understanding the technologies in order to evaluate their suitability. In some instances, regulators are collaborating with industry to facilitate the appropriate development of RegTech. They are not validating the solutions offered; rather, they are creating a climate favourable to the development of this industry.

The UK FCA's approach is to encourage firms to adopt RegTech solutions, and to investigate how technology can improve the provider's own efficiency and effectiveness. The UK FCA identifies three broad types of RegTech solutions, including those that i) help firms to meet their regulatory obligations, ii) help regulators to improve their supervisory and market monitoring functions, and iii) help re-shape current regulatory processes and systems.

Because it is mandated to support competition across the sector, the UK FCA is unable to endorse specific solutions. Instead, the authority encourages innovation and collaboration to unlock complexities and reduce costs of regulation in new ways. For example, the UK FCA continues to explore ways to digitise some rules within its handbook to improve the way that firms submit regulatory returns. The UK FCA issued a "call for input" earlier this year and is working with several banks on two pilots to take this work to a production-ready standard by November 2018.

The Australian Securities and Investments Commission's (ASIC) intends to establish a new RegTech liaison group comprising industry, technology firms, academics, consultancies, regulators and consumer bodies. ASIC approach to RegTech includes several activities:

- providing informal assistance to RegTech businesses through the innovation hub
- engaging with the RegTech community (since mid-2016, ASIC has had over 30 meetings with RegTech stakeholders and service providers to better understand their business models and developments)
- performing technology trials, concretely in the fields of cognitive tool to analyse webpages, machine-learning applications assessing document sets, and social media monitoring

Takeaways

RegTech	Supervisors should keep up with regulation technology (RegTech) tools to understand them, evaluate their appropriateness, and interact with the industry to facilitate its development.

CHAPTER 4: INNOVATION HUBS AND REGULATORY SANDBOXES

KEY POINTS

- Reports on supervisory practices in the field of innovation hubs and sandboxes are limited due to the fact that few jurisdictions have fully implemented these tools and implementation has proceeded only in recent years.
- In terms of innovation hubs, 35% of respondent authorities already have one, while another 22% have the capacity and intention to implement one. The main activity of these hubs is to assist market participants who are developing innovative products and services under current regulation. At the same time, they help regulators and supervisors understand market advances in DFPS. Most existing innovation hubs give access both to new market entrants and to those already licensed.
- Sandboxes have been implemented in 22% of jurisdictions, while another 30% of respondents have the capacity and intention to do so. Sandboxes allow participants to test innovative products and services in a controlled environment and, at the same time provide regulators and supervisors with an increased understanding of financial innovation. Those jurisdictions that have already implemented a sandbox presented the potential benefits and barriers they are facing when implementing one. Design, operation, eligibility criteria and disclosure to consumers vary significantly between jurisdictions, while application for the final licenses, periodic reporting and compliance are approached in similar ways.

There are currently no clear and consistent internationally agreed definitions or guiding principles for what constitutes an innovation hub or regulatory sandbox. For the purposes of this chapter, the following general definitions are based on respondents' descriptions of their specific practices:

- **Innovation hub**: a dedicated point of contact within a regulatory agency that provides guidance and assistance to market participants seeking to develop innovative financial products and/or services, to help them navigate existing regulatory frameworks
- **Regulatory sandbox**: a mechanism that enables market participants to develop, test and analyse financial services and/or products in a controlled environment

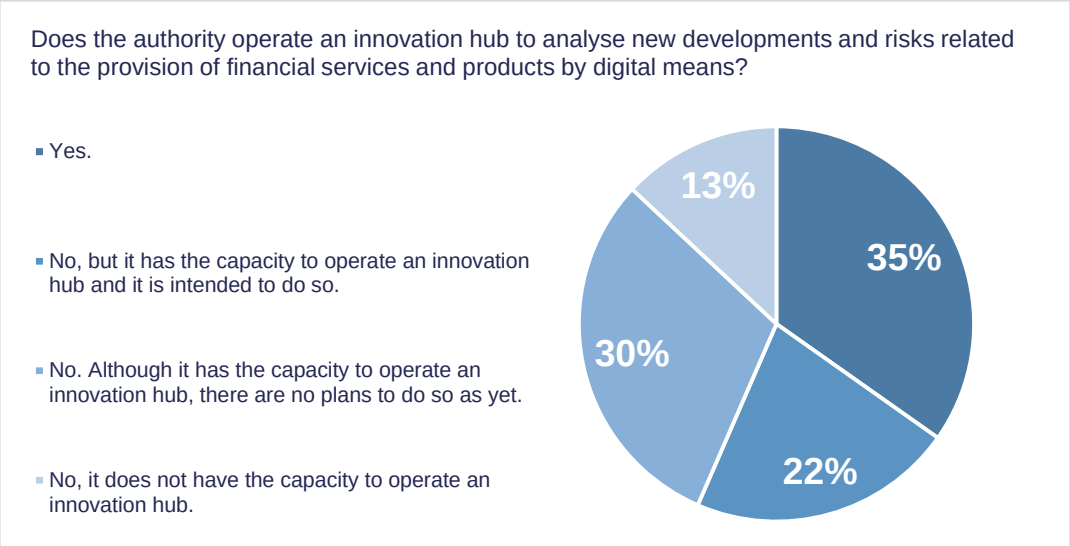
Survey responses indicated the development and implementation of innovation hubs and sandboxes is not widespread, with most practices established within the past two years. This means there is limited data to measure, compare and assess the contributions of these practices to the supervisory framework and the facilitation of innovation within financial services.

The jurisdictions that responded to the survey are only a subset of the jurisdictions that operate innovation hubs and sandboxes, and the responses received are not necessarily reflective of all models and experiences in different jurisdictions. That said, the responses give some indication of the ways different jurisdictions have designed, implemented and are operating innovation hubs and sandboxes.

4.1. Innovation hubs

Approximately 50% of survey respondents have established—or intend to establish—an innovation hub to complement existing regulatory frameworks and support the development of innovative financial services and/or products.

Graph 8 Respondents that have established or intend to establish an innovation hub



Purpose and activity

Survey responses indicated that supervisory bodies have generally designed their innovation hubs to provide guidance and assistance to market participants who seek to develop innovative financial products and/or services to navigate existing regulatory frameworks. These hubs:

- provide a streamlined service for market participants and reduce perceived barriers to innovation within existing regulatory frameworks to foster and accelerate innovation within financial services
- increase supervisory bodies' understanding of the regulatory issues arising from the development of innovative financial products and services

Respondents noted that hubs were largely managed by internal committees, taskforces, study groups or fora, with some respondents noting their committees or fora include external representatives (e.g., other regulatory agencies, industry associations, universities and industry participants).

Digital innovations that have been, or are currently under consideration by innovation hubs include block chain, other DLT, mobile on-boarding and digital automation.

One respondent plans to start gathering information from market participants (including banks and other financial intermediaries) on major projects they have designed to manage the shift towards digitalisation and their attitudes towards FinTech.

Other respondents have begun to explore the development of RegTech by examining how regulatory requirements and technology could converge to provide efficiencies and streamline compliance.

Eligibility requirements

Eligibility requirements for access to innovation hubs vary among respondents, with eligibility aligned to the purpose of the hub—for example, facilitating market participation by FinTech start-ups or fostering innovation more broadly. Most models gave access to new market entrants and/or FinTech start-ups and other FinTech-related businesses. Some respondents also gave access to existing licensed market participants.

The development and implementation of innovation hubs as a supervisory practice is still very much in its infancy. For this reason, there are few case studies and/or relevant statistics to indicate the successes (or otherwise) of the hub's contribution to their regulatory frameworks and the facilitation of innovative products and services. Some respondents were also unable to provide detailed information due to confidentiality restrictions. Even with these limitations, some respondents were in a position to share initial statistics and findings.

The Netherlands AFM indicated that its innovation hub had received over 200 approaches from market participants between 2016 and 2017. Participants sought guidance on various topics, including data, licensing, block chain, electronic identification and the revised PSD2. They were from diverse market sectors including payment and investment institutions, insurance, intermediaries, banks, crowdfunding businesses and RegTech-related companies.

The Australian Securities and Investments Commission (ASIC) indicated it had worked with 240 entities, 206 of which have received informal assistance and held over 183 meetings with FinTechs and other stakeholders. Australia has also granted 39 new financial service and credit licences, as well as 12 variations. Statistics show their hub engagement has led to a 36% reduction in the time it takes to get a license.[9]

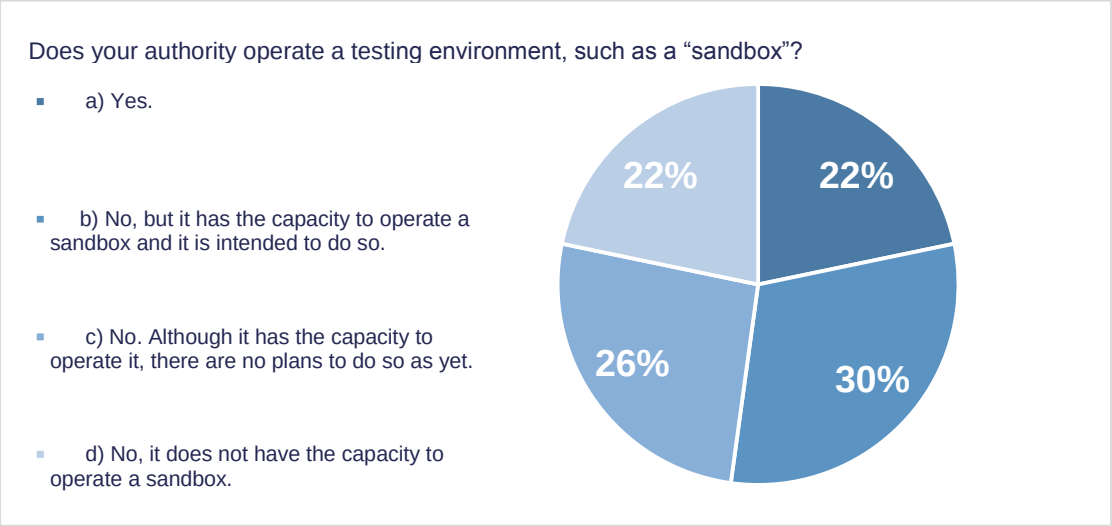
As innovation hubs mature, increased empirical data may become available to help assess their contribution to the regulatory framework and how they facilitate innovation in financial services.

4.2. Sandboxes

Approximately 50% of survey respondents have established—or intend to establish—a regulatory sandbox to enable market participants to develop, test and analyse innovative financial services and/or products with real consumers, while operating within a controlled environment.

[9] The most recent available information is that ASIC has worked with 326 entities, 287 which have received informal assistance. This has resulted in 63 new financial service and credit licenses and 16 variations.

Graph 9 Respondents that have established or intend to establish a regulatory sandbox



Purpose and approaches

Survey responses indicated that a range of sandbox models are operating within the global marketplace. Although diverse in nature, each model has been structured to give eligible participants an opportunity to test innovative financial services and/or products with real consumers in the market while remaining within the regulatory framework and/or under a form of regulatory supervision. Implementing a sandbox has the potential to facilitate and foster financial innovation by:

- increasing understanding of financial innovation and its interplay with current regulatory frameworks
- meeting changing consumer needs in a safe and timely manner

Respondents who currently operate or intend to operate a sandbox, were asked to name the primary goal of the sandbox in the context of the supervisory body's regulatory mandate.

Table 11 Potential benefits in implementing a sandbox

Potential benefits	Key considerations
Foster innovation	Rapidly evolving consumer needs stimulate the development of innovative, timely and agile solutions. Businesses may reduce the time and cost of testing products, bringing their innovations to the market in a faster and more cost-effective manner.
Promote fair competition	A sandbox may increase and promote competition in innovative products and services, to the benefit of consumers, and reduce the burden faced by firms in navigating potentially complex regulatory frameworks that may not have been established with these new products in mind.
Promote financial stability	Sandboxes encourage new market participants, who may be unaware as to whether and how their products and services may be regulated, to engage with the regulator and test the viability and/or feasibility of their products within an adapted regulatory environment. This enables supervisors to gain a better understanding of how these new products and services operate and may impact the broader economy.

Potential benefits	Key considerations
Enhance consumer protection, improving the supervision	Supervisory bodies may work collaboratively with innovators from the beginning of the product-development cycle, ensuring consumer protection is built in and tested robustly. Supervisory bodies have an opportunity to: • gain a deeper understanding of innovative products and services in the market through increased access to a broader range of product offerings • assess the impact of rules and regulations on innovative products before creating new regulations designed to address how best to supervise or regulate those products • develop closer relationships with new and emerging market participants
Favour financial inclusion	DFPS may promote financial inclusion by reducing transaction costs, whether those arise from physical barriers such as distance from financial centres or from access to information.

Survey responses indicate the primary goal in establishing a sandbox was to foster innovation. One respondent stated that promoting financial stability was the main purpose and another respondent indicated their sandbox was designed to achieve three goals in equal measure: to foster innovation, ensure consumer protection while improving supervision, and promote financial inclusion. This respondent indicated that other authorities in its jurisdiction were responsible for the promotion of fair competition and financial stability.

Barriers to implementation

Implementing a sandbox is not without risk. Table 12 summarises some potential barriers and key considerations identified by respondents.

Table 12 Potential barriers and key considerations in implementing a sandbox

Potential barriers	Key considerations
Competition concerns	Should a sandbox compromise a level-playing field, competition may be adversely affected, violating neutrality principles (e.g. access is not open to all market participants or some participants are eligible for certain waivers while others are not). Some respondents give the upmost importance to ensuring all market participants are subject to the same regulatory requirements.
Jurisdictional issues (e.g. state-federal/regional)	Jurisdictions that regulate financial services at both a state and federal/regional level may encounter significant challenges when attempting to design and implement a sandbox across all levels in a timely and consistent manner.
Supervisory risks	Supervisory bodies could be held liable by consumers, or be perceived to be liable, where a sandbox participant engages in misconduct, is negligent, and/or fails to the detriment of a consumer. The likelihood of this occurring may increase where a sandbox participant is not required to notify consumers that they are purchasing a product or service in a test environment and/or the supervisory body does not take an active role in, or closely supervise the sandbox.
Resourcing	Supervisory bodies may not be adequately resourced (e.g. lacking experienced staff or requisite technology) to operate a sandbox, particularly sandboxes designed to operate across multiple market sectors.

Potential barriers	Key considerations
Amendments to the regulatory framework	A significant majority of respondents who did not have an active sandbox indicated that doing so would require varying degrees of amendments to their existing regulatory frameworks. Respondents who indicated that amendments would not be required typically had frameworks in place with discretionary legislation under which a regulatory sandbox could be introduced.

On balance, most respondents saw potential value in implementing a sandbox to foster innovation by complementing their existing regulatory frameworks. However, not all supervisory bodies considered a sandbox an appropriate solution.

Design

The design and operation of sandboxes varied widely among respondents, with significant variation in the degree of sandbox oversight and management by the relevant supervisory body.

For example, the Netherlands AFM indicated that prospective products are considered on a case-by-case basis by the relevant supervisory body, determines whether, how and under what conditions the sandbox is to be put in place for each applicant. The product is then tested for a pre-agreed period of time, during which the supervisory body monitors the sandbox and has the discretion to change or constrain how it operates. At the end of the test period, the supervisory body must decide whether the sandbox has to be adapted, can stay in force indefinitely or should be discontinued.

In contrast, other respondents, such as Autorité des marchés financiers du Québec (AMF) and Australia ASIC, may take a more limited role in sandbox oversight and management and may choose not to monitor sandbox participants during the test period. In these circumstances, eligible sandbox participants must generally meet all standard regulatory requirements that may apply, subject to any exemptive relief granted.

Exemptive relief may include caps or limits placed on the products and/or services to be tested, the maximum amount of funds involved and the number of consumers with whom sandbox participants may engage during the test period. In some jurisdictions, participants must apply upfront for relief to participate in the sandbox; in others, participants are only required to notify the relevant supervisory body, provided all other relevant criteria are met.

Some respondents fell between these two approaches, taking a slightly more hands-on role during the test period, but not maintaining continual oversight.

At the end of the test period, most sandbox participants are required to apply for a financial services licence or authorisation if they intend to continue to provide the tested financial services and/or products. Generally, sandbox participants are not automatically entitled to tailored authorisations or licences, and some jurisdictions, such as Indonesia OJK, have established time limitations which require participants to apply for a licence or authorisation within a set time period (e.g., within one year after the end of the test period).

Many respondents said that extensive information on the sandbox participant's operational model and service and product offering(s) was gathered during the test period. Therefore, the participant's licence application may require less information and assessment than is normal, potentially creating licensing efficiencies.

Key design features in most sandbox models included:

a. eligibility criteria
b. periodic reporting
c. compliance
d. complaints management and redress
e. disclosure

a. Eligibility criteria

Meeting eligibility criteria to access the sandbox is a key design feature for most sandbox models. However, the type of access given varies significantly from broad access (e.g. access is available to all market participants) to restricted access, where access is only available to certain sectors and types of business (e.g. start-ups or P2P lenders).

Most respondents indicated their sandbox is also subject to a wide range of other eligibility criteria. For example, UK FCA has eligibility criteria that include the following. Each financial service or product must:

- be innovative in nature
- be of benefit to the public or specific classes of consumers
- require some form of relief from existing policy or legal barriers
- be sufficiently developed to be fit for use in a realistic environment

The Australian Securities and Investments Commission noted that its eligibility criteria include restrictions that exclude incumbent players and their related entities or representatives, as well as all persons banned from providing financial or credit services in its jurisdiction. This jurisdiction allows foreign companies to access the sandbox if the company is already registered as a foreign company under the supervisory body's legislative framework.

b. Periodic reporting

Periodic reporting by sandbox participants is central for most sandboxes that are currently operational, although reporting obligations vary in nature and frequency and are still under development in some jurisdictions.

The Australian Securities and Investments Commission indicated the sandbox participant must provide a report to the supervisory body within two months of the end of the test period, including:

- the number of consumers who purchased a product or service during the test period
- the number and nature of complaints received and handled
- the number and nature of complaints escalated to external dispute resolution

The report must also include:

- general information about consumer demographics
- a description of the issues identified or faced during the test period and how those issues were resolved
- a description of the regulatory requirements identified as barriers to viability
- revenue and expense information

Indonesia OJK indicated that specific information must be provided by particular participants (P2P lenders) in the course of their operations, from initial registration with the sandbox until they subsequently obtain a licence (one-year period). This includes:

- directors' roles and responsibilities
- IT and electronic systems management
- data and information management
- electronic system security
- incident handling and reliability
- product and services information disclosure

c. Compliance

All respondents who currently operate a sandbox have supervisory practices and tools in place to ensure that sandbox participants comply with the pre-determined operating conditions of the sandbox.

Some respondents indicated the regulatory tools used to ensure compliance outside of the sandbox are also applied to sandbox participants (e.g. surveillance, enforcement action). Other respondents' sandbox design incorporates ongoing liaison with, and monitoring of the sandbox participant during the test period. Some respondents indicated participants may apply for a financial service licence or authorisation while they are in the sandbox, which would also provide a way to assess compliance.

Regardless of the compliance monitoring framework, participants who fail to comply with the operating conditions of the sandbox may have their access terminated during the test period.

d. Complaints management and redress

Survey responses indicated that in some cases, complaints management and consumer compensation obligations have been incorporated as a condition of participating in the sandbox.

The Australian Securities and Investments Commission indicated that to operate in the sandbox, participants must maintain a process for handling complaints, including membership with an external dispute resolution scheme, so that consumers have adequate options for recourse in the event of a complaint or dispute. Participants must also have in place "adequate compensation arrangements" to compensate consumers for losses or damage suffered if the participant fails to comply with its obligations or engages in any misconduct.

e. Disclosure

Respondents are currently using divergent approaches as to whether sandbox participants are required to inform consumers that the financial services and/or products being provided are being done so under test conditions:

- **Required to inform**: sandbox participants must inform relevant consumers that the financial service and/or product is being provided under test conditions and/or under a licensing exemption. Participants must note that some of the standard consumer protections the consumer would ordinarily receive from a licenced market participant

may not apply. However, in some jurisdictions, the requirement to inform may only apply depending on the level of risk and/or tests planned by the participant.

- **Not required to inform**: sandbox participants are not required to specifically inform consumers that the financial service and/or product is being provided under test conditions. However, participants will generally remain subject to standard requirements that apply in the ordinary course of business (e.g. disclosure and conduct obligations) and additional requirements may be imposed if required.

Supervisory practices

As with innovation hubs, the development and implementation of regulatory sandboxes as a supervisory practice is still very much in its infancy: most sandboxes were recently established. There are few case studies and/or relevant statistics to indicate the successes (or otherwise) of the sandbox's contribution to their regulatory framework and the facilitation of innovation. Two respondents provided initial statistics and/or case studies:

UK FCA: assessment of sandbox implementation

UK FCA published a report in October 2017 reflecting its experiences in its sandbox's first year. It found the sandbox met a genuine demand in the market and was encouraged by its initial findings. The insights from the tests so far suggest the sandbox is providing the potential benefits it set out to achieve, including reducing time and cost of getting innovative ideas to market, ensuring greater access to finance for innovators, and ensuring appropriate safeguards are built into new products and services. UK FCA noted that it had supported 60 firms out of 207 applications received across its first two cohorts. Indicators of success included:

- 75% of firms accepted into the first cohort have successfully completed testing
- around 90% of firms that completed testing in the first cohort are continuing toward a wider market launch following their test

The majority of firms issued with a restricted authorisation for their test have gone onto secure a full authorisation following completion of their tests. Of those accepted into the second cohort, 77% of firms have progressed toward testing. FCA anticipates that a similar proportion of the second cohort will take these propositions to market as it has experienced in the first cohort.[10]

Autorité des marchés financiers du Québec (AMF) noted it had granted limited relief to an entity that operates an online platform offering services (including facilitating venture capital and angel investing) to start-ups operating in the technology sector. Limited relief was granted from certain obligations and prospectus requirements for two years[11].

AMF noted that implementing the sandbox has increased their understanding of some challenges faced by market participants seeking to launch innovative products; these include entry barriers (e.g., regulatory gaps and/or issues with the existing framework). Netherlands AFM indicated it had increased its understanding of associated risks, perceptions of supervisory bodies, and misunderstandings of the regulatory framework by compliance and/or legal personnel. The Australian Securities and Investments Commission noted their

[10] See Financial Conduct Authority, *Regulatory sandbox lessons learned report*, October 2017 (PDF, 317.29 KB).
[11] See Ontario Securities Commission, Securities Law & Instruments, Angellist, LLC and Angellist Advisors, LLC, 24 October 2016.

sandbox had helped them develop relationships with the financial and RegTech communities.

As with innovation hubs, more empirical data are likely to become available over time to help assess sandboxes' contribution to the regulatory framework and to facilitating innovation in financial services.

Takeaways

On balance, survey responses indicated there is value in individual supervisory bodies considering whether to introduce innovation hubs and sandboxes to increase their understanding of financial innovation and its interplay with current regulatory frameworks and to address changing market conditions in a timely manner.

These potential benefits must be carefully considered against potential risks, including any inconsistencies or distortions such practices may introduce into the marketplace in the context of the specific market and regulatory framework in each jurisdiction. Given that the balance between facilitation of innovation and the appropriate management of risk is delicate and specific market/regulatory contexts are quite diverse, individual supervisory bodies may prefer other supervisory practices or approaches.

Supervisory bodies may wish to monitor the development of innovation hubs and sandboxes. As these supervisory practices develop and mature, more empirical data will become available to measure and assess their respective contributions to the supervisory framework, the facilitation of innovation in financial services and the consequent benefits to consumers. They will also provide jurisdictions with useful case studies for consideration in the context of their own jurisdictions and mandates.

Innovation hubs and Sandboxes	There is value for supervisors in considering whether to introduce innovation hubs and sandboxes to increase their understanding of financial innovation, its interplay with current regulatory frameworks, and to address changing market conditions in a timely manner. But these potential benefits must be carefully assessed against potential risks, taking into consideration the regulatory set-up of each jurisdiction.

RESPONDENT AUTHORITIES

Jurisdiction	Respondent authority
Australia	Australian Securities and Investments Commission (ASIC)
Brazil	Central Bank of Brazil (BCB)
Canada	Financial Consumer Agency of Canada (FCAC)
Canada	Autorité des marchés financiers (AMF), province of Québec
Chile	Central Bank of Chile (CBC)/ Superintendency of Banks and Financial Institutions (SBIF)
France	Autorité de contrôle prudentiel et de résolution (ACPR)
Germany	Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)
Indonesia	Otoritas Jasa Keuangan (OJK)
Ireland	Central Bank of Ireland
Italy	Central Bank of Italy
Japan	Financial Services Agency (FSA)
Korea	Financial Services Commission (FSC)/ Financial Supervisory Service (FSS)
Lithuania	Bank of Lithuania
Luxembourg	Financial Sector Surveillance Commission (CSSF)
Mauritius	Bank of Mauritius
Netherlands	Netherlands Authority for the Financial Markets (AFM)
Norway	Financial Supervisory Authority
Peru	Superintendency of Banking, Insurance and Private Pension Funds Administrator (SBS)
Portugal	Banco de Portugal
Romania	National Bank of Romania
Russia	Central Bank of Russia
South Africa	South African Reserve Bank (SARB)
Spain	Banco de España
United Kingdom	Financial Conduct Authority (FCA)

GLOSSARY

AI Artificial Intelligence

AGM Annual general meeting

AML/CTF Anti-money laundering/combating the financing of terrorism

App Application

COBIT Control objectives for information and related technology

DFPS Digital financial products and services

DLT Distributed ledger technology

EBA European Banking Authority

E-Money Electronic money

EU European Union

FinCoNet International Financial Consumer Protection Organisation

FinTech Financial technology

ISACA Information Systems Audit and Control Association

ISO International Organization for Standardization

IT Information technology

MoU Memorandum of understanding

NIST National Institute of Standards and Technology

OECD Organisation for Economic Cooperation and Development

PSD2 (EU) Payment Services Directive 2

P2P Peer-to-peer

RegTech Regulatory technology

SupTech Supervisory technology

VC Virtual Currencies

DEFINITIONS

Term	Definition
Consumer	Individuals acting for personal, domestic or household purposes, not business purposes.
Consumer credit	Credit provided to individuals for personal, domestic or household purposes, and not business purposes. This includes both secured credit (such as mortgage loans and personal loans) and unsecured credit (such as lines of credit, credit cards, overdraft facilities, payday lending and micro-finance).
Crowdfunding	Open calls to the public to raise funds for a specific project. In its typical form, an online platform gathers fund seekers (project owners) and fund givers (backers). Project owners publicise their requests for funds via the platform to contact potential backers. Crowdfunding models are generally grouped into four types: a) donations, b) rewards, c) lending (crowdlending), and d) investment (crowdinvesting).
Digital financial products and services (DFPS)	Financial products and services commercialised by bank or non-bank institutions through digital channels (online or mobile), i.e., products and services made available to clients namely through the internet (browser), mobile phones, smartphones, tablets or apps. DFPS can encompass various monetary transactions such as depositing, withdrawing, sending and receiving money, as well as other financial products and services including payment, credit and savings. DFPS can also include non-transactional services, such as monitoring personal financial information through digital devices[12].
FinTech	Technologically enabled financial innovation that could result in new business models, applications, processes or products, with an associated material effect on financial markets and institutions and the provision of financial services.
Innovation hub	A dedicated point of contact within a regulatory agency that provides guidance and assistance to market participants who seek to develop innovative financial products and/or services to navigate existing regulatory frameworks.
Jurisdiction	The territory over which the respondent's supervisory authority is exercised.
RegTech	New technologies used to meet regulatory requirements, address regulatory changes and enhance risk management automatically, more effectively and efficiently.
Regulatory sandbox	A mechanism that enables market participants to develop, test and analyse financial services and/or products in a modified regulatory environment.
SupTech	Application and use of innovative or cutting-edge technology by supervisors to carry out their supervisory and surveillance work more effectively and efficiently (e.g. big data usage, machine learning).
Supervisory tools and practices	Instruments, procedures and devices used by supervisors to ensure that supervised entities comply with the applicable regulation and best practices (e.g., reporting information, complaints handling, on-site inspections, mystery shopping). The same tool can be implemented and used differently, according to each supervisory authority's practice.

[12] OECD, 2017, G20/OECD INFE Report on ensuring financial education and consumer protection for all in the digital age, p.14

LIST OF REFERENCES

Alex Lipton, David Shrier, Alex Pentland. Connection Science & Engineering. Massachusetts Institute of Technology (MIT), 2016, *Digital Banking Manifesto: The End of Banks?* available at https://cdn.www.getsmarter.com/career-advice/wp-content/uploads/2016/12/mit_digital_bank_manifesto_report.pdf

Alliance for Financial Inclusion (AFI), 2014, *Consumer Protection in Mobile Financial Services* available at https://www.afi-global.org/sites/default/files/publications/mfswg_guideline_note_7_consumer_protection_in_mfs.pdf

Bank for International Settlements (BIS), 2018. *Sound Practices: Implications of fintech developments for banks and bank supervisors* available at https://www.bis.org/bcbs/publ/d431.pdf

Bank for International Settlements (BIS), 2018. Financial Stability Institute. *FSI Insights on policy implementation No 9 Innovative technology in financial supervision (suptech) – the experience of early users.* https://www.bis.org/fsi/publ/insights9.pdf

Banque de France - Financial Stability Review No. 20, 2016, *Financial Stability in the digital era* available at https://publications.banque-france.fr/sites/default/files/medias/documents/financial-stability-review-20_2016-04.pdf

Bart van Liebergen – Associate Policy Advisor of Institute of International Finance, 2017, *Machine Learning: A Revolution in Risk Management and Compliance?* available at https://www.iif.com/system/files/32370132_van_liebergen_-_machine_learning_in_compliance_risk_management.pdf

Board of Investment Mauritius (BOI), 2016, *Regulatory Sandbox License Guidelines* available at http://www.investmauritius.com/media/389644/Guidelines-RSL.pdf

Centre for European Policy Studies - European Credit Research Institute (CEPS and ECRI), 2017, *The Future of Retail Financial Services. What policy mix for a balanced digital transformation?* available at https://www.ceps.eu/system/files/TFRFutureFinancialServices.pdf

Committee on the Global Financial System (CGFS) and the Financial Stability Board (FSB), 2017, *FinTech credit. Market structure, business models and financial stability implications* available at http://www.fsb.org/wp-content/uploads/CGFS-FSB-Report-on-FinTech-Credit.pdf

De Nederlandsche Bank (DNB) and Autoriteit Financiële Markten (AFM), 2016, *More room for innovation in the financial sector. Market access, authorisations and supervision: Next steps* available at https://www.afm.nl/en/nieuws/2016/dec/maatwerk-innovatie

European Banking Authority (EBA), 2017, *Discussion Paper on the EBA's approach to financial technology (FinTech)* available at http://www.eba.europa.eu/documents/10180/1919160/EBA+Discussion+Paper+on+Fintech+(EBA-DP-2017-02).pdf

European Central Bank (ECB), 2017, *Guide to assessments of fintech credit institution licence applications* available at https://www.bankingsupervision.europa.eu/legalframework/publiccons/pdf/licensing_and_fintech/ssm.guide_on_assessment_for_licensing_of_fintech_credit_insts_draft.en.pdf

European Commission, 2017, *Consultation document: Fintech: A More Competitive and Innovative European Financial Sector* available at https://ec.europa.eu/info/sites/info/files/2017-fintech-consultation-document_en_0.pdf

European Parliament, 2017, Report on FinTech: the influence of technology on the future of the financial sector (2016/2243(INI)) available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2017-0176+0+DOC+PDF+V0//EN

Financial Conduct Authority (FCA), 2017, *Regulatory sandbox lessons learned report* available at https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf

Financial Stability Board (FSB), 2017, *Financial Stability Implications from FinTech Supervisory and Regulatory Issues that Merit Authorities' Attention* available at http://www.fsb.org/wp-content/uploads/R270617.pdf

International Monetary Fund (IMF), 2017, *Fintech and Financial Services: Initial Considerations* available at https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2017/06/16/Fintech-and-Financial-Services-Initial-Considerations-44985

International Organization of Securities Commissions (IOSCO), 2017, *IOSCO Research Report on Financial Technologies (Fintech)* available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf

Jaime Caruana, General Manager of Bank for International Settlements (BIS), 2016, *Financial inclusion and the fintech revolution: implications for supervision and oversight* available at http://www.bis.org/speeches/sp161026.htm

Mark Carney, Governor of the Bank of England, 2017, *The Promise of FinTech – Something New Under the Sun?* available at http://www.bankofengland.co.uk/publications/Documents/speeches/2017/speech956.pdf

Monetary Authority of Singapur, 2016, *Fintech Regulatory Sandbox Guidelines* available at http://www.mas.gov.sg/~/media/Smart%20Financial%20Centre/Sandbox/FinTech%20Regulatory%20Sandbox%20Guidelines.pdf

OECD, 2017, *G20/OECD INFE Report on ensuring financial education and consumer protection for all in the digital age* available at http://www.oecd.org/daf/fin/financial-education/G20-OECD-INFE-Report-Financial-Education-Consumer-Protection-Digital-Age.pdf

OECD, 2018, *G20/OECD Policy Guidance on Financial Consumer Protection Approaches in the Digital Age* available at http://www.oecd.org/finance/G20-OECD-Policy-Guidance-Financial-Consumer-Protection-Digital-Age-2018.pdf

OECD, 2018, *G20/OECD INFE Policy Guidance on Digitalisation and Financial Literacy* available at http://www.oecd.org/finance/G20-OECD-INFE-Policy-Guidance-Digitalisation-Financial-Literacy-2018.pdf

Ontario Securities Commission, Securities Law & Instruments, *Angellist, LLC and Angellist Advisors, LLC*, 24 October 2016. Available at http://www.osc.gov.on.ca/en/SecuritiesLaw_ord_20161024_angellist.htm

Roelof Goosen, former Director of Financial Inclusion at the National Treasury of South Africa, for the G20 Global Partnership for Financial Inclusion (GPFI), 2017, *Building Inclusive Digital Payments Ecosystems: Guidance note for governments* available at https://www.gpfi.org/sites/default/files/documents/GPFI%20Guidance%20Note%20Building%20Inclusive%20Dig%20Payments%20Ecosystems%20final_0.pdf

UK Government Chief Scientific Adviser, 2015, *Distributed Ledger Technology: beyond block chain* available at http://www.ameda.org.eg/files/gs-16-1-distributed-ledger-technology.pdf

World Economic Forum, 2017, *Beyond Fintech: A Pragmatic Assessment Of Disruptive Potential In Financial Services* available at http://www3.weforum.org/docs/Beyond_Fintech_-_A_Pragmatic_Assessment_of_Disruptive_Potential_in_Financial_Services.pdf