Deutsche Bank

EU Transparency Register ID Number 271912611231-56

Basel Committee on Banking Supervision
Centralbahnplatz 2
CH-4002 Basel
Switzerland

Deutsche Bank AG
Winchester House
1 Great Winchester Street
London EC2N 2DB

Tel +44 20 75458000
Direct Tel +44 20 75451903

31 October 2017

Consultative document on Sound Practices: Implications of fintech developments for banks and bank supervisors

Dear Sir / Madam,

Deutsche Bank welcomes the opportunity to comment on the Basel Committee on Banking Supervision's (BCBS) consultation on the implications of FinTech on banks and bank supervisors.

Deutsche Bank supports the BCBS's efforts to identify and assess risks and related supervisory challenges associated with technology-driven innovation in financial services ('FinTech'), and share the objective of ensuring the entire banking system is subject to comprehensive and effective regulations and oversight. A regulatory framework which promotes consistent standards based on regulated activities will ensure resilient markets and consistent protections for consumers.

In our view a key risk for supervisors and banks relates to inconsistent design or application of regulatory and supervisory requirements to different types of entities providing similar services in financial markets. In this regard, we strongly support regulatory initiatives, such as recent work by the European Banking Authority and the European Central Bank, to identify and address potential gaps and unregulated entities providing financial services within their jurisdictions. To ensure consistency in approach and avoid the risk of regulatory gaps and arbitrage, it is also important regulators coordinate globally.

Deutsche Bank is clear on the importance of robust bank risk management processes to address new technologies and outsourced activities. Irrespective of the outsourced service, banks must carefully select external service providers that are fit and proper for the performance of the tasks delegated to them. This is true for FinTech, but also for other traditional technology providers.

Equally important for the identification and management of risks from FinTech however is the continued engagement and learning by regulators to keep pace with technological innovation. In this regard, we strongly support the development of regulatory sandboxes to enhance shared learning across public and private sector market participants. Regulator involvement in sandbox testing will help to better inform regulatory decisions on the application of proper rules / oversight for new models.

Finally, it is important also to recognise the potential for technological innovations to enhance the safety and soundness of banks, as well as assist supervisors in carrying out their tasks.

FinTech and FinTech companies should be understood as potential partners in addressing risk as well as possible sources of risk themselves.

Detailed comments on the recommendations made within the consultative document are set out in the attached document. Please do not hesitate to contact us if you have questions or wish to discuss these issues further.

Yours faithfully,

Matt Holmes
Head of Regulatory Policy

Observation 1: The nature and the scope of banking risks as traditionally understood may significantly change over time with the growing adoption of fintech, in the form of both new technologies and business models. While these changes may result in new risks, they can also open up new opportunities for consumers, banks, the banking system and bank supervisors.

Recommendation 1: Banks and bank supervisors should consider how they balance ensuring the safety and soundness of the banking system with minimising the risk of inadvertently inhibiting beneficial innovation in the financial sector. Such a balanced approach would promote the safety and soundness of banks, financial stability, consumer protection and compliance with applicable laws and regulations, including anti-money laundering and countering financing of terrorism (AML/CFT) regulations, without unnecessarily hampering beneficial innovations in financial services, including those aimed at financial inclusion.

Deutsche Bank supports the focus on ensuring a balanced approach. Care must be taken to ensure an innovation-friendly environment which does not compromise market integrity and fair competition. In this regard, we support a principles based approach for regulating FinTech, along the lines of that proposed by the European Commission in its March 2017 publication 'FinTech: A More Competitive and Innovative European Financial Sector'[1]. In this publication the European Commission outlined three key principles to inform an approach to regulation of FinTech: i) technological neutrality; ii) proportionality; and iii) market integrity.

Of these principles DB has argued that market integrity should take precedence over proportionality in determining the future policy framework. Proportionality should not come at the expense of proper risk management practices; care must be taken to ensure consistent incentives to manage risks and protect consumers. This is particularly important for standards governing cybersecurity, AML/CFT and data and consumer protection. Innovation will not occur, and the opportunities identified by BCBS will not materialise, if consumers lose trust as a result of inconsistent protection, or the system as a whole is weakened by gaps in regulation. The principle of 'same service, same rules' should be applied to secure consistent standards, avoid regulatory arbitrage amongst market players and allow competition to be conducted on a level playing field to mitigate risks from newly adopted technologies.

It is also important that regulators should look beyond their borders when developing or updating regulatory frameworks to address FinTech innovation. A key lesson of the financial crisis was that a globally interconnected financial system requires a globally consistent regulatory framework. This insight should inform the regulatory response to FinTech developments, both to mitigate the risk of regulatory arbitrage, but also to avoid regulatory barriers and costs acting as a barrier to new market entrants. Global coordination will ultimately provide for both more efficient and secure standards for cross-border FinTech activities.

In order to be in a position to identify new and emerging risks, regulators will need to have a strong degree of monitoring and transparency across FinTech activities. Monitoring of all market participants providing financial services, whether bank or non-bank, will be an important element of this, but given the pace of innovation and limited regulatory resources, ensuring effective industry dialogue and establishing fora for discussion with a broad range of market participants will also be important. This is already happening across some jurisdictions, but there is scope for further coordination and structure at the international level.

[1] https://ec.europa.eu/info/sites/info/files/2017-fintech-consultation-document_en_0.pdf

RegTech

In relation to the BCBS's assessment of RegTech, Deutsche Bank agrees that the effective deployment and application of RegTech could be used to improve compliance processes at financial institutions and pursue regulatory objectives. We also agree that innovation should not come at the expense of safety and soundness or consumer protection. However, in order for the potential benefits of RegTech to be realised, there are a number of other conditions which will need to be fulfilled. Examples of these include consistency around data requirements and legal frameworks for distributed ledger technology (DLT) and other technologies:

- **Reference data and standardisation:** The implementation of DLT for trade reporting would benefit from the provision of a golden source of reportable instruments under various items of regulation, such as MiFID II in Europe. Regulation should also specify standardisation across fields[2] to enable automated aggregation of data across jurisdictions or group subsidiaries.

- **Legal framework for blockchain technology:** A robust legal architecture, with an appropriate dispute resolution mechanism and governing principles, is required to facilitate further development and implementation of blockchain programs currently in development. From a cross-border perspective, the regulatory framework for blockchain will need to address issues on: the institutional roles and interaction between market infrastructure players; legal certainty for securities holdings and transactions (including settlement finality); laws dealing with ownership and transfer; issuer and investor protection; appropriate market access; interoperability; and identity verification.

- **Cyber risk:** Security standards around regulator connectivity to distributed ledgers (for regulatory reporting and market oversight purposes) will need to be carefully designed to mitigate data protection and cyber risks. Regulators may become a target of cyber-crime given their broad access to the ledger data. Access would therefore need to be strictly view-only and only addressed in a permissioned ledger set up.

  Fragmentation of data localisation requirements on what should be categorised as private, confidential or of national interest under different jurisdictions' cybersecurity laws presents additional challenges. International level agreement on common data sets and their categorisation would promote the consistent treatment of data and protections, and facilitate organisations' compliance with common data privacy standards.

- **KYC standards:** As highlighted in the recent paper from the Bank for International Settlements[3], KYC utilities could reduce the cost and administrative burden associated with customer due diligence processes. However, regulatory action is needed to support the establishment of standards for systems / controls of such utilities (ideally adopted at the global level), to ensure accuracy of the utility-held data and where liability rests in the case of erroneous data or standards not being met. These standards could be developed directly by regulators or by an industry body, subject to regulatory approval. An external accreditation process to test compliance with this standard would also benefit the utilities' integrity.

[2] Examples include the Legal Entity Identifier, Product Identifier and Customer Identifier
[3] http://www.bis.org/cpmi/publ/d147.pdf

Observation 2: For banks, the key risks associated with the emergence of fintech include strategic risk, operational risk, cyber-risk and compliance risk. These risks were identified for both incumbent banks and new fintech entrants into the financial industry.

Recommendation 2: Banks should ensure that they have effective governance structures and risk management processes in order to identify, manage and monitor risks associated with the use of enabling technologies and the emergence of new business models and entrants into the banking system brought about by fintech developments. These structures and processes should include:

- robust strategic and business planning processes that allow banks to adapt revenue and profitability plans in view of the potential impact of new technologies and market entrants;
- sound new product approval and change management processes to appropriately address changes not only in technology, but also in business processes;
- implementation of the Basel Committee′s Principles for sound management of operational risk (PSMOR) with due consideration to fintech developments; and
- monitoring and reviewing of compliance with applicable regulatory requirements, including those related to consumer protection, data protection and AML/CFT when introducing new products, services or channels.

Banking Models

Sound new product approval and change management processes within banks will play an important role in maintaining standards and protecting consumers, or 'de-risking innovation.' However, regulators will also play a key role in de-risking this evolution. The application of proportionate regulations based on an entity's business activities, as explained in our response to Observation 1, will allow new and existing firms to compete and succeed based on the value delivered to consumers.

As stated above FinTech innovation has the potential to improve the safety and soundness of incumbent banks through improved operational, cost and post-trade efficiencies[4], automated KYC and AML processes, and other benefits outlined by BCBS in Observation 1.

FinTech firms can also provide new partnership opportunities which are mutually beneficial and may help to develop new markets, not just compete for existing business. Conversely, FinTech firms are able to deliver new products to a broader customer base, more efficiently by being able to make use of existing banking and payments infrastructures.

Deutsche Bank is pragmatic in its choice of FinTech solutions and we seek to apply them wherever significant value is generated. These solutions are adopted through various means, such as through business and technology groups, our internal innovation labs, industry consortia and direct investment in FinTech companies.

We are also actively working to build a platform to provide a wider service-offering (i.e. including capabilities from FinTech firms partners) to our clients in addition to our existing FinTech partnered solutions[5].

[4] For example by reducing the settlement cycle for various instruments – this would reduce counterparty risk exposures for derivatives transactions by shortening the margin period of risk (MPOR) and also free up bank capital earmarked for longer MPORs

[5] For example: gini (voice scanning); WebID Solutions (video authentication); Fincite (robo advice); and DSwiss (eSafe)

Cyber risk

Given the interconnectedness of the financial system, an appropriate and uniform end-to-end security level is needed along the complete financial services value chain to ensure robust cybersecurity resilience. A connected system is only as secure as its weakest link.

Existing initiatives addressing the financial sector, including the Directive (EU) 2016/1148 ('NIS Directive') or the EBA Guidelines on ICT Risk Assessment under the SREP 2017, as well as local implementation such as BaFin's coming Minimum Requirements on Banking-IT ('BAIT') in Germany, create a broad and robust cybersecurity regulation for banks, irrespective of the type of FinTech engagement. These initiatives cover a range of topics, from IT strategy and governance to the management of IT risks, security and user authorisation, amongst others.

The application of FinTech in financial services must follow the same established high security standards that incumbent financial services firms use. In Europe, for example, this includes requirements set forth in the NIS Directive, General Data Protection Regulation (GDPR), Payments Services Directive 2 (PSD2), and the Committee on Payments and Market Infrastructures (CPMI) and International Organisation of Securities Commissions (IOSCO) Guidance on cyber resilience for financial market infrastructures.

Requirements on security incident reporting to regulators, such as those defined in PSD2 and the NIS Directive, should also apply across market participants including FinTech firms and third-party providers. Furthermore, banks should be informed of security breaches / incidents at connected FinTechs in case their customer data is affected to allow for appropriate follow-up measures and notifications. To ensure cybersecurity standards are maintained as the financial services landscape evolves and new technologies adopted, regulators should actively engage with new and existing market players to understand emerging trends and address any potential regulatory and/or enforcement gaps.

Cyber risk may also be mitigated through the use of technology sandboxes. For example, our Deutsche Bank Labs initiative provides a robust platform for identifying, engaging and testing new and emerging FinTech technologies. The Labs offer a consistent, risk managed entry point to the firm's business and technology teams, where potential business opportunity may be defined and validated. Regulatory sandboxes, as explained further in our response to Observation 7, provide opportunities for early identification of cyber, and other operational risks, stemming from the use of new technologies, products or services.

Deutsche Bank welcomes the continued focus of regulators on addressing cyber risk and encourage continued engagement with cybersecurity practitioners to learn and share best practices. A cybersecurity framework that encourages a risk-based approach, global coordination and sharing of cyber threat information would best serve to protect the integrity of the financial system. Deutsche Bank strongly supports the G20 initiative to enhance cross-border cooperation and cyber resilience of financial institutions and infrastructures, and the FSB's recent analysis of publicly released cybersecurity regulations, guidance and supervisory practices[6].

[6] http://www.fsb.org/wp-content/uploads/P131017-2.pdf

Observation 3: Banks, service providers and fintech firms are increasingly adopting and leveraging advanced technologies to deliver innovative financial products and services. These enabling technologies, such as artificial intelligence (AI)/machine learning (ML)/advanced data analytics, distributed ledger technology (DLT), cloud computing and application programming interfaces (APIs), present opportunities, but also pose their own inherent risks.

Recommendation 3: Banks should ensure they have effective IT and other risk management processes that address the risks of the new technologies and implement the effective control environments needed to properly support key innovations.

Deutsche Bank fully agrees with the importance of having effective IT and other risk management processes to address the risks of new technologies. These processes, as with regulations, are most effective when applied in a technology-neutral and risk-based manner. Irrespective of the technology to be adopted, appropriate controls and governance processes must be implemented to ensure prudent risk management.

Below we provide our thoughts on the specific technologies highlighted by BCBS, their risks and the role regulators can also play in managing these risks in future:

AI / robotics / machine learning

In the field of AI and machine learning ('algorithms'), we see four main risk categories at present: i) the appropriateness of data ('data risks'); ii) the algorithm's logic; iii) the risks arising from the interactions of algorithms that may not be adequately foreseen ('algorithm-interaction risks'); and iv) legal and data privacy risks from inappropriate use of data.

While banks' internal processes should address risks within their reach and authority (e.g. risk of badly coded algorithms), there may be a need for third-party oversight to manage unforeseen outcomes that can arise from the interactions of different algorithms. This interaction risk was observed in the 2010 NASDAQ 'flash crash', which saw the automated execution of a large sell order trigger extreme price movements. The effect was found to be especially impactful if the algorithm did not take price into account. According to the joint US agency report[7], the interaction between automated execution programs and algorithmic trading strategies can quickly erode liquidity and result in disorderly markets.

Ongoing regulatory efforts to clarify the criteria and controls related to 'profiling'[8], such as the recent guidelines published by the Article 29 Data Protection Working Party[9], are very welcome. Regulatory certainty in this area will support consistent standards across all market players and will help to protect consumer.

Blockchain and Distributed Ledger Technology (DLT)

The technological risks and relevant controls can be substantively different between blockchain, as a subset of the family of DLT, and other DLTs. For example, while the concept of 'high availability' and disaster recovery should be equally applied across the DLT category, the details can differ. Blockchains – especially those with native tokens – would require additional risk management considerations such as: the number of nodes (minimum, down-time, add or remove); computational power requirements (depending on the consensus mechanism); where to locate the nodes; crypto key renewal; revocation; and management, etc.

[7] https://www.sec.gov/news/studies/2010/marketevents-report.pdf
[8] automated processing of personal data to evaluate personal aspects such as performance at work or economic situation
[9] http://ec.europa.eu/newsroom/document.cfm?doc_id=47742

In this regard, the various applications of blockchain and DLT underscore the importance of principles-based regulatory risk management standards. This approach will best accommodate business models emerging now and in the future, and provide a responsible balance between risk management and practical benefits from innovative DLT solutions.

Deutsche Bank encourages regulators to continue to engage with market participants in order to understand the implications of emerging DLT solutions. This will help inform the development of appropriate regulatory and supervisory actions. Direct regulatory participation in pilot programs could also help clarify the minimum controls for a DLT based system to be brought to market. This may include minimum standards on information security, and business and design controls.

Cloud

The availability of cloud technologies provides clear benefits in terms of improved performance and cost efficiency. However, to date uncertainty around the application of existing outsourcing requirements to the cloud services business model has acted as a break on broader adoption. The highly standardised vendor arrangements which characterise cloud service providers (CSPs) are different from the customised relationships that are typical for other vendors used by banks, and for which existing guidance was designed.

Deutsche Bank therefore strongly supports regulatory efforts, such as the draft recommendations on cloud outsourcing issued by the European Banking Authority (EBA)[10], to provide increased regulatory certainty in this area. Importantly, regulatory clarity and harmonised standards will help to enhance risk management practices for outsourcing across market participants and jurisdictions.

Regulators at national and global levels should collaborate with cloud service providers (CSPs) and financial institutions in order to continue to refine these requirements and harmonise supervisory expectations. To enable effective risk management practices, regulators should also ensure that unnecessarily prescriptive, or duplicative requirements are avoided and that the overall approach remains proportionate and outcome focused.

We would also encourage regulators to consider alternate approaches which reduce potential burdens without diluting risk control. For example, moving towards regulator-driven shared assessments of CSPs on behalf of a consortium of banks would be greatly beneficial from both control and cloud adoption perspectives. This will be especially useful as only a small subset of CSPs are large enough to service the scale of activities outsourced by financial institutions. Given this potential concentration risk, direct regulator involvement will help to ensure compliance with regulatory requirements, and secure the necessary contractual rights for financial institutions to support robust oversight and transition planning.

Direct engagement by regulators with CSPs to develop standardised terms that fulfil regulatory requirements has also been undertaken in recent years. This approach was used by the Dutch Central Bank with Microsoft in 2013 to make audit rights available within the Netherlands. In Singapore, the industry is moving towards a standardised certification called the Outsourced Service Provider's Audit Report (OSPAR) which is based on the Association of Banks in Singapore (ABS) Outsourced Service Provider Guidelines[11]. This system allows CSPs to be certified once against a common template / set of requirements and reduces the need for duplicate certifications by outsourcing institutions. OSPAR also requires that outsourcing

[10] https://www.eba.europa.eu/documents/10180/1848359/Draft+Recommendation+on+outsourcing+to+Cloud+Service++%28EBA-CP-2017-06%29.pdf
[11] https://abs.org.sg/industry-guidelines/outsourcing

institutions receive ongoing assurance of the operational effectiveness of controls which are discrete between the institution and the CSP.

Observation 4: Banks are increasingly partnering with and/or outsourcing operational support for technology-based financial services to third-party service providers, including fintech firms, causing the delivery of financial services to become more modular and commoditised. While these partnerships can arise for a multitude of reasons, outsourcing typically occurs for reasons of cost-reduction, operational flexibility and/or increased security and operational resilience. While operations can be outsourced, the associated risks and liabilities for those operations and delivery of the financial services remain with the banks.

Recommendation 4: Banks should ensure they have appropriate processes for due diligence, risk management and ongoing monitoring of any operation outsourced to a third party, including fintech firms. Contracts should outline the responsibilities of each party, agreed service levels and audit rights. Banks should maintain controls for outsourced services to the same standard as the operations conducted within the bank itself.

Banks are already subject to a range of regulations covering outsourcing which address both outsourced services and related risk management. In the EU this includes, amongst others, EU Directive 2014/65 ('MiFID II, especially its Article 16) in conjunction with Commission Delegated Regulation (EU) 2017/565 (especially its article 31) or EU Directive 2011/ 61/EU ('AIFMD', especially its Article 20) in conjunction with Commission Delegated Regulation (EU) No 231/2013 supplementing Directive 2011/61/EU (especially Art 75 and sections 89 and 111).

Taken together these Directives set out detailed requirements covering the proper selection, supervision and governance of external service providers to avoid undue additional operational risk. Irrespective of the outsourced service, banks must carefully select external service providers that are fit and proper for the performance of the tasks delegated to them. Appropriate controls and governance processes must be implemented to ensure prudent risk management, including audits, as well as the continued supervision by the competent supervisory authorities. Outsourcing of important operational functions may not be undertaken by banks in such a way as to materially impair the quality of its internal control and the ability of the supervisor to monitor the firm's compliance with all obligations.

Deutsche Bank employs a robust Vendor Risk Management Framework ('Framework') and process that reviews each outsourcing provider in accordance with relevant regulatory and policy requirements. This includes a Service Risk Assessment and Vendor Risk Assessment to determine what standard controls need to be in place to meet the requirements of key control functions, including Information Security Risk, IT Vendor Risk, Business Continuity Management and Group Data Protection, to name a few. These requirements are based on the services being provided to the Bank by the supplier.

The Third Party Management and the overarching Framework are applied to all vendors – irrespective of whether a traditional or new FinTech service provider – using a risk-based approach to assess vendor risk, based on the standard service that is being provided to the Bank. Against each service, the control function defines the control standards and the standard artifacts the vendor needs to provide to evidence the control is in place.

The Framework is applied well before a supplier service is 'live'; i.e., being delivered into the Bank. The average Vendor Risk Assessment takes about four months to complete; however, this varies by supplier responsiveness, service and complexity of the sourcing contract. The

Framework is designed and deployed with enough lead time to ensure control gaps are identified and mitigating actions plans in place to address the gaps in line with the risk the gap creates. Any gap creating a potential regulatory breach must be closed before the service is allowed to go live.

To further support these processes, and given the increased importance of FinTech and start-up technology companies, Deutsche Bank has strengthened the connectivity between its third party risk management function and our internal innovation labs to ensure each external FinTech firm is aware of the process and applicable requirements at an even earlier stage.

Observation 5: Fintech developments are expected to raise issues that go beyond the scope of prudential supervision, as other public policy objectives may also be at stake, such as safeguarding data privacy, data and IT security, consumer protection, fostering competition and compliance with AML/CFT.

Recommendation 5: Bank supervisors should cooperate with other public authorities responsible for oversight of regulatory functions related to fintech, such as conduct authorities, data protection authorities, competition authorities and financial intelligence units, with the objective of, where appropriate, developing standards and regulatory oversight of the provision of banking services, whether or not the service is provided by a bank or fintech firms.

For the reasons set out in our comments on Recommendation 1 greater cooperation and coordination across prudential and conduct authorities, public authorities and supervisors, is of critical importance. Guidance from international standard setters would also be beneficial in helping to coordinate approaches by those authorities responsible for overseeing areas of regulation which may intersect with FinTech related risk in the banking system (e.g. broader corporate or data privacy regulation). A good example in this respect would be security incident reporting obligations under the EU NIS Directive, which could also be triggered under other regulatory regimes such as data protection laws or local regulations. This may lead to a situation that one minor incident must be reported to some authorities, but not to other authorities with deviating thresholds and reporting times leading to high administrative efforts just implementing and tracking all applicable rules and notifications.

Observation 6: While many fintech firms and their products – in particular, businesses focused on lending and investing activities – are currently focused at the national or regional level, some fintech firms already operate in multiple jurisdictions, especially in the payments and cross-border remittance businesses. The potential for these firms to expand their cross-border operations is high, especially in the area of wholesale payments.

Recommendation 6: Given the current and potential global growth of fintech companies, international cooperation between supervisors is essential. Supervisors should coordinate supervisory activities for cross-border fintech operations, where appropriate.

Deutsche Bank welcomes this recommendation and strongly supports enhanced international cooperation between supervisors. Given the global operations of financial institutions and the expected global growth of FinTech firm activities, cross-border regulatory coordination and certainty is necessary to maximise the potential benefits, increase the safe scaling of FinTech services and address common inherent risks from innovative solutions. Efficient coordination will provide entities of all sizes with clarity on local regulations / supervisory expectations applicable to new business models, and assist regulators in their assessment of potential regulatory gaps from new market players and technologies.

This could be achieved through a formal cooperation mechanism between regulators in different jurisdictions[12]. These cooperation mechanisms have already been developed between some authorities and could be further developed to: enable regulators to refer FinTech firms and other market participants to regulatory counterparts in other jurisdictions; enhance information sharing on financial services innovation between regulators and market participants; and coordinate cross-border projects to test innovative products and processes.

Observation 7: Fintech has the potential to change traditional banking business models, structures and operations. As the delivery of financial services becomes increasingly technology-driven, reassessment of current supervision models in response to these changes could help bank supervisors adapt to fintech-related developments and ensure continued effective oversight and supervision of the banking system.

Recommendation 7: Bank supervisors should assess their current staffing and training models to ensure that the knowledge, skills and tools of their staff remain relevant and effective in supervising new technologies and innovative business models. Supervisors should also consider whether additional specialised skills are needed to complement existing expertise.

Broader uptake of Fintech solutions will result in greater demand for new skills and technological knowledge across all market participants. If the regulatory framework is going to keep pace with developments and supervisors are going to be in a position to effectively monitor risks, then public authorities may end up competing for the same expert resources. In such a scenario enhanced dialogue between regulators and market participants will be all the more important in order to mitigate the impact of resource constraints that may arise. Ongoing dialogue between regulators and market participants would greatly benefit this effort. Regulator-led fora, such as the European Commission's proposed 'Innovation Academy', which will foster the exchange of information between organisations and authorities is one example of how this might work in practice.

Direct support for, and participation in, bank pilot programs would also prove highly beneficial. Regulatory sandboxes which allow testing of new technologies should provide an opportunity for regulators to develop staff skills and understanding of market developments. Sandbox initiatives have been launched across various jurisdictions, including Singapore, Australia and the UK, in an effort to accelerate the development of innovative solutions and improve regulators' understanding of developing technologies. As noted in the UK Financial Conduct Authority's (FCA) first annual report on its regulatory sandbox[13], testing in the sandbox 'allows [the FCA] to observe more closely the potential risks DLT may present and to feed into these tests to ensure appropriate safeguards are in place and potential consumer detriment is minimised.' Furthermore, regulatory sandboxes would support the ongoing training of staff directly with the organisation and enhance communication with supervised entities.

[12] Examples of cooperation mechanisms which may serve as a potential template include agreements between the UK Financial Conduct Authority (FCA) and the Monetary Authority of Singapore (MAS); the FCA and Hong Kong Monetary Authority (HKMA); the MAS and the Autorité de Contrôle Prudentiel et de Résolution (ACPR) and the Autorité des Marchés Financiers (AMF) of France

[13] https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf

Observation 8: The same technologies that offer efficiencies and opportunities for fintech firms and banks, such as AI/ML/advanced data analytics, DLT, cloud computing and APIs, may also improve supervisory efficiency and effectiveness.

Recommendation 8: Supervisors should consider investigating and exploring the potential of new technologies to improve their methods and processes. Information on policies and practices should be shared among supervisors.

Deutsche Bank supports supervisors' efforts to explore the potential applications of RegTech and supervisory technology ('SupTech'). Examples include data mining algorthims to assist with the aggregations and analysis of data submitted by financial institutions, computer modeling and forecasting for stress testing, amongst others.

The creation of RegTech sandboxes – or establishment of a separate component within broader sandboxes – would help promote further development and mutual learning of potential RegTech use cases and implementation challenges. This may take the form of a secure testing environment directly at the regulator, which would allow testing of promising use cases. Direct market participant and regulator interaction could benefit the shared learning of new technologies and potentially speed up adoption of new processes. The US Commodity Futures Trading Commission (CFTC) recently announced such an initiative as part of its "LabCFTC" function. Cross-border collaboration would also be useful to allow proof of concept and testing to take place on an international border basis.

Observation 9: Current bank regulatory, supervisory and licensing frameworks generally predate the technologies and new business models of fintech firms. This may create the risk of unintended regulatory gaps when new business models move critical banking activities outside regulated environments or, conversely, result in unintended barriers to entry for new business models and entrants.

Recommendation 9: Supervisors should review their current regulatory, supervisory and licensing frameworks in light of new and evolving risks arising from innovative products and business models. Within applicable statutory authorities and jurisdictions, supervisors should consider whether these frameworks are sufficiently proportionate and adaptive to appropriately balance ensuring safety and soundness and consumer protection expectations with mitigating the risk of inadvertently raising barriers to entry for new firms or new business models.

Ongoing review of regulatory and supervisory frameworks is essential to ensure that they remain fit for purpose and are able to adapt to innovation within the market. In completing these review cycles regulators should seek to achieve proportionate rules that facilitate competition and new developments, however, this should not be done at the expense of market integrity.

The aim must be to provide a level playing field for all market participants, employing a 'same service, same rules' principle. As noted in our response to Observation 1, standards around AML/CFT, data protection, cybersecurity and consumer protection in particular should be applied consistently across all market participants.

Such an approach will help avoid regulatory arbitrage and ensure risks stemming from the provision of financial services activities are properly addressed, irrespective of the provider.

Observation 10: The common aim of jurisdictions is to strike the right balance between safeguarding financial stability and consumer protection while leaving room for innovation. Some agencies have put in place approaches to improve interaction with innovative financial players and to facilitate innovative technologies and business models in financial services (e.g. innovation hubs, accelerators, regulatory sandboxes and other forms of interaction) with distinct differences.

Recommendation 10: Supervisors should learn from each other's approaches and practices, and consider whether it would be appropriate to implement similar approaches or practices.

As stated in our response to Observation 7, Deutsche Bank strongly supports the creation of regulatory sandboxes for the purposes of testing new business models against existing regulations and laws. We also support the sharing of key non-confidential regulatory and legal aspects of 'lessons learned' from sandbox experiments with other sponsors of similar proposals. This would help mitigate the risks of competitive divide between those with resources to conduct sandbox experiments and those with low resources but with plausible good concepts and ideas.

Coordination across these initiatives would be beneficial for banks, new entrants and regulators to share information on uses cases, collaborations and discuss areas of regulatory uncertainty which may serve as a barrier to further developments and implementation of new technologies. Rapid syndication of learning across platforms and national regulators would provide a significant value to market participants and regulators alike.

Regulators should also seek to foster greater participation in sandboxes and not restrict access to innovators or businesses of certain sizes or experience levels, and need to be sensitive to resource availability of applicants. This will help to promote fair competition and eliminate uncertainty on whether incumbent institutions that partner with start-ups may participate in sandbox initiatives.

In addition, supervisors should engage directly with FinTech companies and incumbent digital innovation functions to experience first-hand the 'digital first' approach to working practices and how this may underpin corporate culture.