October 30, 2017

Mr. William Coen
Secretary General
Basel Committee on Banking Supervision
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland

Re: Consultative Document – Sound Practices: Implications of fintech developments for banks and bank supervisors

Dear Mr. Coen:

The Institute of International Finance and its members ("IIF") appreciate the opportunity to comment on the Basel Committee on Banking Supervision (BCBS)' consultation paper (the "Consultation") "Sound practices: Implications of fintech developments for banks and bank supervisors". The global emergence of financial technology (fintech) will alter the shape of the financial sector in the years to come. Reaping the full benefits from these innovations in the financial system will require a coordinated global regulatory approach that balances the promotion of innovation and experimentation while guarding against the migration of existing risks and the emergence of new risk types.

In the below, we will first present the IIF's key messages regarding the emergence of fintech and its implications for banks and bank supervisors, and then respond in more detail to each of the BCBS' observations and recommendations.

IIF key messages

1. The Basel Committee's attention to fintech and its implications for banking regulation and supervision is welcome. This, however, needs to be part of an overall, **cross-sectoral approach under the leadership of the Financial Stability Board (FSB)**, drawing from regulators and policy makers from banking, securities, insurance, and other financial areas. Coordinating policy outside the boundaries of traditional banking and even financial regulation may also become increasingly important as digital finance operates in a data driven economy where privacy and cyber policy make a progressively significant impact on the industry. Such developments will require a comprehensive policy framework.[1]

2. The rapid development of fintech will certainly have significant repercussions for both financial

[1] Financial Stability Board, "Financial stability implications from fintech: Supervisory and regulatory issues that merit authorities' attention," June 27, 2017.

firms and their regulators/supervisors. The BCBS set of observations and sound practices should adopt a more **balanced approach**, as it tends to primarily focus on potential new risks for incumbent banks but does not delve sufficiently deep on the significant implications for non-bank entities outside of the purview of the Basel Committee's regulatory and supervisory remit, where many potential risks could originate, or on aspects not related to prudential supervision.

3. The evolving nature of technological innovation will require a **regulatory and supervisory approach that is sufficiently flexible, adaptable, risk-based, holistic and cross-border in nature** to fully be able to address emerging risks without stifling innovation. Such approach should have such characteristics as:

    a. **Risk-Based**: The diverse nature of new technologies (and fintech), encompassing a multitude of business plans, products, and services, gives rise to a similarly diverse set of risks and issues. Any new regulatory framework or requirement to address the emergence of fintech/tech/Ecommerce in the financial services space should be graduated, risk-based and expand the regulatory perimeter to include activities and risks regardless of their business model. Indeed, there are specific activities that do warrant careful attention by regulators, regardless of what type or size of institution is engaging in the activity, such as payments, lending, investments and data collection/storage.

    The risks associated with these activities have far reaching impacts to consumers and the broader financial system (i.e. money laundering, terrorist financing, disparate impact, fraud, identity theft, unauthorized transfers, etc.), and should be subject to consistent regulation and supervision. A risk-based approach is best-placed to identify and capture activities that may migrate from traditionally regulated sectors to less or non-regulated entities. It should be built on the clear principle that similar risks should be regulated and supervised in a similar way, and with oversight tied to the scale of the activity and the risks presented rather than the party involved.

    Effectively developing a risk-based approach to regulation and supervision will require that standards be set by the FSB, which coordinates policies for the entire financial sector, rather than focusing on specific types of entities. It would also imply that supervision and regulation would not address "fintech" as separate from incumbent institutions: the framework, through its focus on risk, would be agnostic to the type of business model or entity involved in it.

    b. **Flexible and principles-based –** As technological innovation changes business models and activities in the financial sector, regulators and supervisors should ensure that their practices and regulations effectively address risk regardless of the status of the underlying technology or method used to execute that activity. This requires that they be principles-based and forward-looking. In contrast, detailed and prescriptive

regulations risk becoming obsolete as new technologies change the way the regulated activity is conducted.

c. **Holistic in Nature**: Effective regulation and supervision of fintech will require expanding the focus to policy issues that are not traditionally associated with financial sector supervision, such as cybersecurity, data use and privacy. Proper coordination with non-financial regulators should be addressed, as well as the consistency of financial regulatory regimes with non-financial ones.

d. **Cross-Border**: Regulatory and supervisory approaches should be international in nature and be based on close cross-border cooperation. This would prevent regulatory arbitrage, forum shopping and fragmentation of regulatory approaches.

4. **Addressing data gaps** through improved collection and sharing of information will be key in bridging existing information gaps on the risks posed by new entities, business models and technologies, their size, growth and exposures to different markets, and their impact on the structure and evolution of local and global financial networks. Such an approach could follow the example of previous FSB Data Gaps and Shadow Banking initiatives.

5. Meeting customer expectations, expanding access to finance, and managing risk increasingly rely on the **ability to access and analyze data from both traditional as well as new sources**. Incumbent institutions should not be held back from developing these data capabilities and keeping pace with new entrants into the financial ecosystem.

6. The entry of **large e-commerce and digital platforms (sometimes called "bigtech") may have far-reaching implications for the financial system in terms of structure and stability, and for its clients in terms of privacy and data issues**. Due to the scale and global reach of these firms and their unrivaled access to non-traditional consumer data sources, these firms could rapidly gain systemic importance. The consequences of such transformation for the system could be difficult to manage from a supervisory perspective unless supervisors and regulators adapt ex ante. A level playing field between banks and large e-commerce firms on the use of data can help ensure that customers receive the full benefit of these innovations in financial services.

7. Similarly, the entry of smaller (start-up) fintech firms should be closely monitored. **Smaller firms may lack the necessary scale and infrastructure to develop appropriate AML, cybersecurity and risk controls**. Their interconnectedness with other institutions could cause risks at these firms to spread through the financial system.

8. We appreciate that the consultation paper recognizes the opportunities offered by new technologies to attain efficiencies and sound risk management, and believe that emerging regulatory and supervisory approaches should recognize that **the benefits of adopting new technologies at incumbent institutions outweigh the associated risks**. While we agree that the

implementation of technology at incumbent institutions needs to go together with rigorous management of associated risks, including to robust implementation controls and governance, it should be recognized that new technologies improve virtually all aspects of FIs' business models: the ability to aggregate and use data for risk management, compliance, lending and strategic uses, and the resilience of IT and data infrastructures to operational and cyber risk. Indeed, an **inability of incumbent institutions to use new technologies to transform themselves is by far the largest strategic risk to the sector** as a whole.

9. We urge regulators, standard setters and supervisors to support **adoption of new technology by Financial Institutions (FIs) as a sound practice**. It could in particular be supported through:
   a. Improving data quality through standardization of formats (such as through the LEI, UPI and UTI)[2], taxonomies and definitions[3], and data sharing arrangements,
   b. Creating international standards for contractual obligations for third-party providers to FIs so that contractual obligations and conditions traditionally applied to outsourced activities (such as audit rights and subcontracting clauses) can be more easily implemented.
   c. Opening innovation channels, such as hubs and sandboxes, to engage both FIs and new entrants working with new technology and new models,
   d. Upgrading reporting portals and methods to create automated sharing mechanisms that accept standardized digital file types.

In addition to these general observations, below we provide answers to some of the questions raised in the consultation as appropriate.

Responses to scenarios and recommendations

BCBS 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.

BCBS 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.

[2] LEI: Legal Entity Identifier. UPI: Unique Product Identifier. UTI: Unique Trade Identifier.

[3] Several examples of differing data definitions complicating data aggregation include: "short term interbank funding" is based on a 3-month horizon for RWA computation in Basel III, while it is based on a "less than one year" threshold in the NSFR. For more information, see IIF, "Regtech in financial services: solutions for compliance and reporting," March 2016. Available at https://www.iif.com/topics/regtech.

IIF Response:

In order to adequately balance risks and opportunities, regulatory frameworks must be forward looking and adaptable to best identify and understand the potential new or changing risks posed by emerging technologies and innovations that are not currently addressed by existing regulatory structures (in line with recommendation 9). The importance of a risk-based approach, under the clear principle that similar risks should be regulated and supervised in a similar way, cannot be over-emphasized.[4] We appreciate that the BCBS recognizes this principle in its paper.[5] To this end, it is imperative that the BCBS work under the auspices of the FSB, together with other sectoral standard setters (including the Committee on Payments and Markets Infrastructures (CPMI), the International Association of Insurance Supervisors (IAIS), and the International Organization of Securities Commissions (IOSCO)) to ensure that regulations address risks equally, regardless of the business model or entity that harbors them. Such an approach would also ensure a fair and balanced competitive market in which actors performing similar activities are regulated in a similar way.

Further, a holistic approach to the design of such a framework is necessary. Risks related to the increasingly interconnected IT ecosystem, such as data use and protection and cybersecurity, must be considered alongside the more traditional consumer, prudential, market and conduct rules already in place. At the same time, it is important that these considerations not stifle the growth of emerging technologies. Given the fast-changing pace of technologies and related business models, we believe it would be beneficial if regulators and supervisors work in partnership with the industry to get an up-to-date view of developments. Further, the cross-border nature of many fintech services should be reflected in cross-border cooperation and coordination among regulators and supervisors in developing regulation and supervisory practices.

Traditionally, licensing and authorization regimes have been key determinants in how different activities are regulated and supervised. Supervisors and regulators should reassess such regimes to see if new business models or technologies warrant inclusion, as is already underway in the EU and US. Given the need for a risk-based regulatory framework that addresses risk in the system equally across different entities, we do not see merit in a separate "fintech" license. Different licensing regimes would create the possibility for a two-tier regulatory environment

[4] We note that several European Union authorities, including the European Commission, European Parliament and ESMA, all support regulation that is "technology-neutral". For example, the Commission has stated that policies should be "technology-neutral to ensure that the same activity is subject to the same regulation irrespective of the way the service is delivered, so that innovation is enabled and level-playing field preserved." (source: https://ec.europa.eu/info/sites/info/files/2017-fintech-consultation-document_en_0.pdf). Similarly , ESMA has stated that "What should be regulated is the provision of a service or an activity independent of the form of the firm providing this service or activity. The aim should be to regulate and supervise entities providing the same type of service on an equal foot." Source: https://www.esma.europa.eu/press-news/esma-news/esma-responds-commission-consultation-fintech.

[5] For example, box 6 says that where "new financial players are reshaping the financial sector, they may be outside the scope of banking sector regulation and subject to less stringent AML/CFT rules than are banks. If not proportionate to the AML/CFT risks, these regulatory gaps or loopholes may lead to some distortion of competition, which may violate the level playing field principle and lead to increased potential for financial crime."

and a risk of regulatory arbitrage.

At the same time, it is important for regulators and supervisors to recognize that the responsible implementation of new technology in itself can also improve the safety and soundness of the system: technologies such as AI, robotics and cloud services can contribute to more effective compliance, risk management and regulatory reporting at financial institutions through better risk data aggregation, money laundering and fraud detection, and early warning systems for credit risk. Replacing legacy IT systems with cloud services, data lakes and APIs can also make institutions' IT and data infrastructures significantly more robust and reliable. Indeed, *lack* of transformation and digitalization in the banking sector is a bigger risk to the sector than transformation itself, threatening the sector's competitiveness and risk management capability.

As discussed in our IIF key messages, regulators can make important contributions to the effective implementation and use of new technology at FIs. Most importantly, and in line with a risk-based approach that treats all entities equally, new entrants and incumbent institutions should have equal opportunity to apply new technologies, and experiment with them through sandboxes, innovation hubs and other innovation-supporting initiatives.

Some of the barriers that banks currently experience on undertaking digital transformation relate to use of digital identity and digital onboarding processes, use of cloud services, prudential rules in some geographies (such as the EU capital frameworks that apply full deduction to software), unbalanced requirements regarding access to data (obliging banks to open their data without similar requirements for other sectors), complex cybersecurity frameworks (with multiple authorities involved), and unbalanced liability frameworks in payment services rules or consumer protection.

Anti-money laundering and counter terrorism financing (AML/CFT)
AML/CFT provides a good example of an area where it is important to reach a proper balance between safeguarding the safety and soundness of the system while supporting financial innovation. New technologies, such as machine learning, are starting to play a key role in flagging and investigating suspicious activity in the financial system – a task that, given the number of (flagged) transactions for institutions to investigate, would benefit greatly from (partial) automation. It is therefore imperative that institutions can apply new technologies to these tasks, subject to appropriate testing, controls, governance and supervision.

Where regulations cause difficulty for innovation, these should be reconsidered. To stay with the example of AML/CFT, KYC utilities could significantly improve AML investigations at financial institutions by enabling them to share relevant information efficiently with each other. However, they are currently not used optimally, as data regulations typically restrict or do not allow institutions to provide or access consumer information cross-border through a third-party provider, thereby inhibiting the effective use of these utilities. Banks will need some assurances that the regulatory, supervisory, and law-enforcement authorities approve of, and will

recognize, the appropriateness of reliance upon any such utility. Without such approval and ability to rely, which is clearly absent in the draft guidance, the incentive to invest in and to use them would be diminished.[6]

BCBS 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.

BCBS 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.

IIF Response:

The IIF and its members agree that banks will need to make sure that they adapt their governance and controls frameworks to account for fintech entrants in the financial system, and ensure robust implementation of the Basel Committee's Principles for sound management of operational risk (PSMOR).

At the same time, how banks internally manage their response to challenges from competing fintechs is ultimately more a commercial issue than a regulatory one, which they should primarily handle in their ability as commercial players in a competitive market, rather than an issue that can be solved through supervision of banks' strategic and business planning processes. With regard to the recommendation that banks should have robust strategic and business planning processes, while we agree with it we would stress that banks have already have robust processes in place in which they typically consider all the factors and information available.

With regard to recommendation 2b, new technologies enable a much faster time-to-market for new products. It is important that the other business processes, especially those related to new

[6] IIF, Letter to the Basel Committee on Banking Supervision, "Re: Revised annex for correspondent banking to the BCBS guidelines on the sound management of risks related to money laundering and financing terrorism," February 22, 2017.

product approval, are not overlooked despite the increased speed of product creation (for example, risk assessment, pricing, compliance, assessments of the suitability of customers, profitability analysis and regulatory reporting).

Another risk that could have a significant impact on financial stability is cyber risk. More than any of the risks mentioned here by the Committee, cyber risk can significantly affect the functions and integrity of all market participants and infrastructure. All players in the system should have adequate controls in place to prevent and deal with such risk given that when it comes to this type of risk, the financial system is only as strong as its weakest link.

BCBS 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.

BCBS 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.

IIF Response: We agree with the Committee's observation that banks and new entrants should have effective IT and other risk management processes to properly support innovation, as well as appropriate processes for due diligence, risk management and ongoing monitoring of outsourced operations. This is a key area of focus for our members. Indeed, to allow for the optimal use of fintech and regtech solutions and to comply with BCBS 239 "Principles for Effective Risk Data Aggregation and Risk Reporting[7]", many institutions have been or are in the process of replacing legacy IT systems (which have often been an amalgamation of many different subsystems) with consolidated operation systems and data architectures based on new technologies such as cloud services, APIs and 'big data' platforms. This has been broadly supported by supervisors.

However, there has also been a general assumption that the automation of internal processes at financial institutions using fintech innovations will necessarily increase the vulnerability of those institutions to cyber and operational risks. We emphasize that this picture is more nuanced in practice, and that technological upgrades generally benefit the robustness of systems:

1. In terms of cyber risk, the assumption of supervisors is that the increased connectivity of new applications will make them more vulnerable to outside, malevolent penetration than existing systems are. However, many existing systems are already connected externally through e-mail, internet, etc. New technologies typically significantly incorporate stronger cryptographic or biometric security guarantees than previous

[7] Basel Committee on Banking Supervision, "Principles for effective risk data aggregation and risk reporting," January 2013.

systems, as it is more likely to conform with current common minimum standards. Indeed, recent cyber-attacks have shown that older software is typically more vulnerable to cyber threats.[8]

2. In terms of operational risk, the assumption is that new technologies bring increased complexity that may be difficult to manage for FIs. Again, this is not necessarily true. Newer systems are typically more compatible with other systems, and are often used to consolidate a range of older systems, thereby decreasing systems complexity and typically decreasing the probability of failure. A consolidated system also allows for easier and faster detection and resolving in case a system failure happens.

It is important that regulators recognize the potential benefits of new technologies in banking, and the fact that they outweigh the associated risks. Indeed, rather than digitalization itself, an inability of incumbent institutions to use new technologies to transform themselves is the largest strategic risk to the sector as this would hamper their ability to compete and to manage risks.

As discussed in our key messages, we emphasize that regulators can best take an active role in supporting the effective implementation and use of new technologies within financial institutions for risk management, compliance, regulatory reporting and commercial/competitive purposes.

In terms of Cloud computing, the European Banking Authority's draft document of "Recommendations on outsourcing to cloud service providers" defines how to assess the materiality of cloud outsourcing and creates a tool for exercising the right to audit and its right to access the use of third-party certifications. A definition of pre-Authorized certifications (such as ISO 27001 and SSAE-16) would be welcome in order to include it in the requirements when assessing this kind of providers.

BCBS 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.

BCBS 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.

[8] See, for example, the WannaCry attack, which exploited weaknesses in the outdated Windows XP operation system.

IIF Response: We agree with the recommendation that banks need appropriate processes to manage their relations with third parties. At the same time, we think that the BCBS' discussion of outsourced activities excludes a couple of key issues:

First, it is important for supervisors to realize that important third-party risks can also come from third parties that do not operate under outsourcing contracts with banks, such as the EU's Payment Services Directive (PSD) II open APIs (based on which account and data aggregators and online lenders can work). These services access bank services by consent of the client rather than the bank. These business models can be a source of operational risk for incumbent institutions, and we believe that there should be more supervisory focused placed on these business models and risks.

Second, existing general outsourcing rules do not fit well with cloud services and other data-related services. These include, for example, the requirement to conduct audits and gain access to the premises. Thereby, the fact that the supply of cloud services is dominated by a few large tech firms with significant market power is changing the relationship between the bank and the outsourcing service provider. Banks may sometimes find it difficult to impose the contractual obligations and conditions traditionally applied to outsourced activities (such as audit rights and subcontracting clauses). We would therefore support creating new rules for cloud providers based on an international framework. Harmonization could contribute to reducing cloud services provider concentration risk, foster market competition among cloud services providers, and enable smoother implementation of clouds across banking groups.

Third, we note that banks already observe the principles outlined in Recommendation 4 when outsourcing to any third party, regardless of whether that is a fintech player or a more traditional type of third-party. In the assessment of outsourcing risk, it is not so much the type of player, but the type of function that is being outsourced which characterizes the associated risk.

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.

IIF Response: As discussed in our key messages, we strongly agree with this recommendation. The emergence of fintech and the potential large-scale entry of bigtech into the market means that supervision and regulation should become:

1. more holistic in scale, encompassing prudential and conduct focus areas as well as competition, data, privacy, financial crime and cybersecurity;
2. risk-based, addressing risk and applying regulatory requirements in a way that is agnostic to the type of business model harboring those risks. This should prevent the migration of risk to, and the emergence of new risks in, low-regulated or non-regulated entities
3. based on close coordination and cooperation among supervisors and regulators to prevent fragmentation of regulation and supervision, and consequent arbitrage and forum shopping by regulated entities.
4. highly adaptable and principles-based, as risks and business models change in tandem with technological innovation and impact on the structure of the financial services market.

Additionally, we believe that the regulatory treatment of data use, sharing, storage and deletion will be key in achieving a level playing field for all participants in the market, ensuring sound lending and risk management practices, and bolstering data security and privacy for consumers of financial institutions and fintechs.

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 for cross supervisory activities -border fintech operations, where appropriate.

IIF Response: We agree with this recommendation and believe that supervision as well as regulation (regardless of whether focused on financial or other aspects of FIs' business models) should be based on close cross-border coordination and cooperation, as many fintech business models operate on web- or app-based platforms, making their services easily accessible across borders. To prevent regulatory arbitrage, forum shopping, fragmentation of regulatory approaches, and to best protect end users in a global environment, supervisors and regulators should cooperate and coordinate their actions.

For supervisors, this means in practice that they could best operate through supervisory colleges and coordination of practices and standards, including non-financial supervisors (such as data and competition authorities). For regulators, coordination of regulatory standards could best take place at the international level, through the FSB, BCBS and other standard setters. Within the EU, such coordination should take place through the Single Supervisory Mechanism (SSM) where applicable, through action by the European Commission, and the European Banking Authority (EBA).

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.

> **IIF Response:** We agree with this recommendation. Effective oversight of new business models and technologies requires that supervisors have a thorough understanding of them, and continue to gain knowledge, skills and staff capacity. Additionally, using these tools in a supervisor or central banks' own operations is probably the most effective way to gain an understanding of their workings, benefits and limits (see our response at recommendation 8).
>
> The use of artificial intelligence and machine learning serves as an example. While this field is closely related to more traditional statistics, the fact that it is based on algorithms and new computer techniques such as distributed computing changes the way models are created, and requires that regulators and supervisors update their understanding of these fields.
>
> Examples of initiatives to bolster supervisors' experience with new technologies and business models could include joint training programs between regulators, banks and fintechs; secondment programs for banks and fintechs to work with regulators and supervisors; and joint industry/regulator groups on specific technologies.

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.

> **IIF Response:** The IIF and its members support this recommendation, and stress that the use of new technologies by supervisors will also improve their ability to audit and supervise the use of those technologies by supervised firms, as it increases their familiarity and understanding of the technology through use. For effective supervision of a financial sector whose technological character is changing rapidly, it is important that supervisors build up adequate knowledge and experience in these fields.

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.

> **IIF Response:** To ensure that risks in the financial sector are appropriately supervised and regulated, it is imperative that regulatory frameworks become risk-based, rather than focused on a particular entity or entities. To prevent the existence of regulatory gaps, supervisors should thereby work to close data gaps through improved and updated collection and sharing of information on new business models, entities and methods.
>
> Further, a review of current frameworks would be beneficial against a backdrop of new technology, innovative business models and evolving risk. New channels and methods may enable regulators, supervisors and licensing bodies to work more effectively with industry while balancing innovation and risk. When considering new approaches, care should be given to design them with consistent principles, as part of a well-conceived continuum of regulatory engagement and supervision, rather than just providing temporary exemption based on the applicant. These frameworks should be globally harmonized wherever possible.

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.

> **IIF Response:** We agree with this recommendation. It is important that regulatory frameworks not only focus on addressing risks, but also promote experimentation, including fintech entrants, and are consistent across different jurisdictions. We therefore support increased harmonization of regulatory initiatives supporting fintech innovation (such as sandboxes and innovation hubs).
>
> It is equally important that these initiatives be open to incumbent players in the financial sector as well as new entrants, as innovation and the adoption of new technology is not limited to new players. In fact, the adoption of new technology at incumbent institutions will be key in bolstering the stability of the sector while going through this technological transformation.

***

The IIF reiterates its appreciation for this opportunity to provide feedback to the BCBS on this important topic. Should you need additional information on this topic please contact me (aportilla@iif.com), Bart van Liebergen (bvanliebergen@iif.com) and Conan French (cfrench@iif.com).

Best regards,

Andrés Portilla
Managing Director, Regulatory Affairs