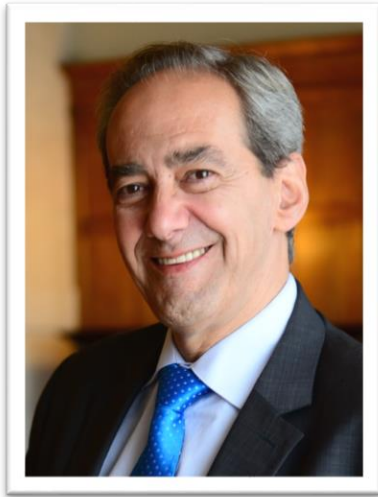




Opportunities and challenges for banking regulation and supervision in the digital age



José Manuel González-Páramo, Executive Board Director BBVA, Chief Officer Global Economics, Regulation and Public Affairs

The digital transformation of the financial sector

The evolution of economy and society is featured by continuous change. Most of the time, this change is slow and incremental but, every now and then, rapid disruptive changes take place in short periods of time, leading to what are commonly known as “revolutions”. We are living now one of these stages of disruption. Massive **adoption of digital technologies** invented in the second half of the 20th century, namely the Internet and mobile phones, together with the exponential growth in computation and storage capacity at a lower cost, is radically transforming the world, **profoundly changing personal relationships, business organisations** and, in general, the way economic value is created.

This **digital revolution has also arrived in the financial sector**. The negative impact of the economic environment on banking, expectations of a prolonged period of low interest rates and the stagnation in lending lead inevitably to the quest for transformation processes that enable costs to be reduced



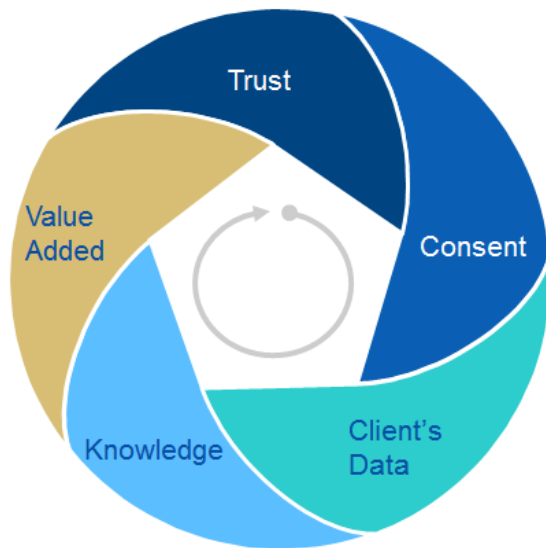
and a boost in revenues. Things become more complicated if we take into account two additional factors: the reputational problems still weighing on banks and the assimilation of the aftermath of the regulatory tsunami. Accepting that all the above requires profound changes in the sector; the presence of this radical disruptive force, the digital revolution, has changed everything.

The disruption characterising the transition in banking is reflected in irreversible changes in two ways. On the demand side, we are already seeing **radical changes in customers**, which have more power than ever. They feel they need to be connected, everywhere, anytime. They also want their needs to be met immediately, including the consumption of relevant and useful content. On the supply side, banking sector is facing **greater competition** from new players coming from the digital world - not only start-ups, but also major digital companies like Google, Amazon or Alibaba- and **technological changes** that will decisively affect the quantity, quality and price of financial services.

In this context of disruptive change, two **forces will be fundamental** for determining the speed of change and the scenario towards which the sector will move. The first, which is internal in nature, concerns the **banks' vision of the future** and their technological, financial and organisational capacity for self-transformation. The second is the **role of the regulators and supervisors** as drivers of or brakes on the changes needed during the transition.

Opportunities and challenges in the digital age

The digitalization of financial services will improve and expand the provision of financial services, contribute to reduce costs and obtain efficiency gains in the system and, ultimately, enable the expansion of the population served, even in rural areas, offering greater speed, convenience and attractiveness. In short, it will take care of their main asset: the **customer trust**, the cornerstone of the digital economy.



“ Without *trust* there is no *data*, without *data* there is no *creation of value* and without *creation of value* there are no *opportunities for people* ”

Figure 1: The virtuous circle of the digital economy

Conversely, despite the aforementioned acknowledged benefits, developments in technology and new market dynamics pose **new opportunities and challenges in efficiency, financial stability, consumer protection and integrity** of the financial sector - key objectives of regulators and supervisors.

- New digital technologies allow banks to obtain multiple efficiency gains: economies of scale, faster time-to-market, higher resilience, speed, flexibility, etc. For example, cloud solutions offer multiple opportunities associated to flexibility and scalability, and allow financial institutions to innovate faster, gain efficiency, reduce time-to-market and improve productivity exponentially.
- From the perspective of financial stability, operational IT and cyber security risks have become a key concern among authorities. Cyber threats may create huge economic damage, but also if there is lack of confidence in the safety and security of digital technologies, the adoption of new technologies will falter even if they offer substantial benefits. For example, automated tools and services, such as electronic trading platforms and robo advisors, may increase the risk of market volatility and procyclicality in stressed or abnormal market conditions.



- In terms of consumer protection, the application of new technologies involves new security risks. Greater access to and use of customers' data increases the relevance of personal data protection. Moreover, some risks arise from automated tools, but they also allow for more control and traceability of the customer relationship.
The use of digital devices (mobile apps), cloud computing or blockchain solutions increase the flow of personal data. Therefore, there is a need to push for strong security measures, such as encryption techniques, and to comply with data location requirements, including international personal data transfers outside the European Union, while securing access to data by competent authorities.
- Finally, regulators and supervisors need to preserve the integrity of the financial system ensuring proper conduct by market participants. For example, the speed of real-time payment systems, the immediate availability of funds and the anonymity may attract illegal economic transactions to real-time payment systems. Similarly, when digital channels are used to acquire and onboard customers, new challenges arise for anti-money laundering and combating the financing of terrorism.

However, it is not all risks for regulators and authorities. Technological advances are also directly helping the industry and the authorities to better address these risks. The so called **“RegTech” solutions** improve risk management functions and facilitate more effective and efficient compliance with regulatory requirements. The potential usage by supervisors of Regtech solution has also been highlighted by De Nederlandsche Bank: “technological innovation offers opportunities for supervisors, for example with respect to the automation of certain supervisory processes”.¹

¹ De Nederlandsche Bank (2017). *Technological innovation and the Dutch financial sector*. Amsterdam: De Nederlandsche Bank. <https://www.dnb.nl/en/binaries/Themaonderzoek%20%20uk_tcm47-336322.PDF>.

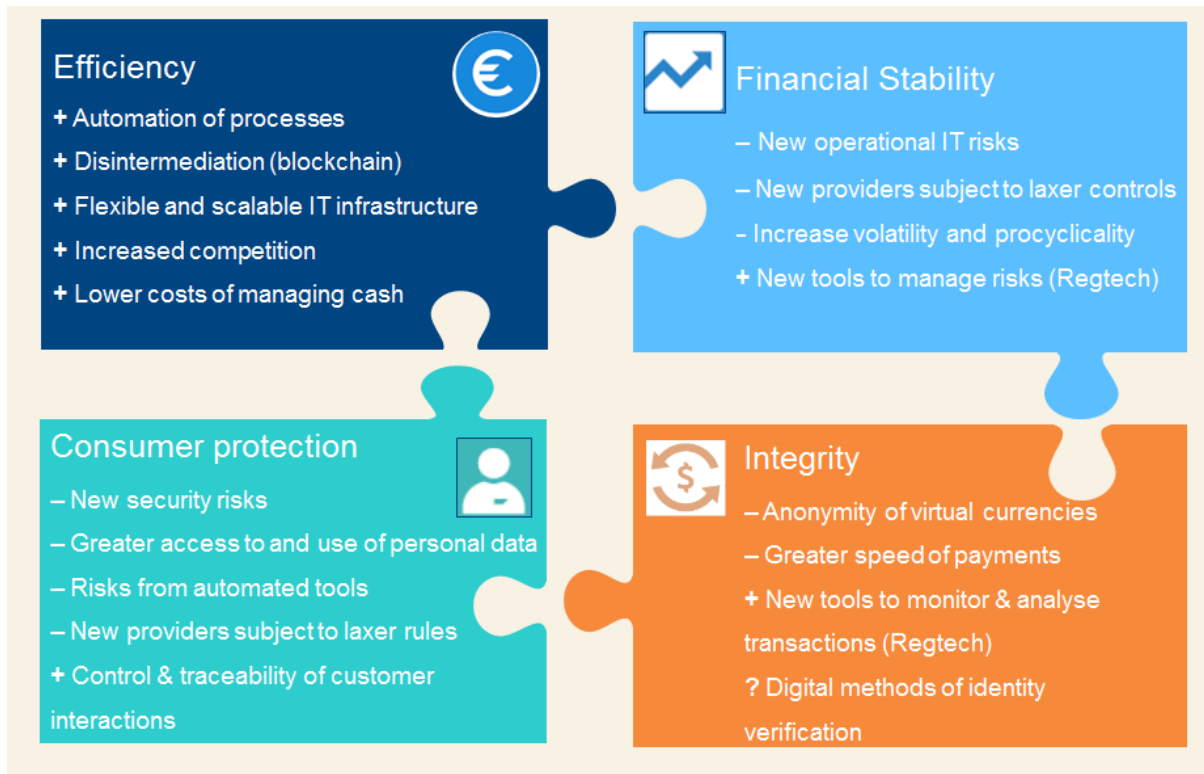


Figure 2: Benefits and challenges for banking regulation and supervision

The aforementioned new challenges, that the digitalization of financial services poses, are **not fully covered by the traditional supervisory and regulatory approach** (mainly focused on capital or liquidity requirements). So regulators and supervisors must tackle them without hindering the transformation of the financial industry.

It is worth highlighting that new digital proposition is at an early stage and it certainly does not pose significant financial stability and consumer risks so far. However, the exponential nature of the new digital infrastructures, business and distribution models and customer solutions allows them to go from “too small to care to too big to fail” in a very short period of time, requiring **authorities to have a far-reaching and anticipated perspective.**



Short- and medium-term regulatory and supervisory priorities

The supervisory and regulatory work ahead is enormous. The question is: Where to begin? **Authorities must combine pragmatism and ambition.** Among all the challenges ahead, there are three key priorities that we must focus on: fair competition, facilitate innovation and cybersecurity.

First, the new digital environment facilitates the emergence of new competitors in the financial landscape. How to properly address these new challenges and ensure **fair competition among the various different providers** of financial services; incumbents, start-ups and major digital players is a major challenge.

In many cases, the concept of “level-playing field” has been used with different, even contradictory, meanings. For some, it means lowering the regulatory barriers to entry in the financial sector, whereas for others new players should be subject to the same obligations that are imposed on banks. The issue is of the utmost importance given the risks involved in providing financial services and consequently, the heavy regulation and supervision to which the sector has always been subject.

Ensuring a fair competition and managing the risks ought to comprise that activities involving the **same risks should receive the same regulatory** treatment, and regulation should **foster innovation removing the unnecessary barriers** to fair competition. To move on from words to deeds, regulatory and supervisory framework should progress on the following fronts:

- **Limiting the implications of prudential regulation** for non-core businesses (i.e. non-deposit-taking activities) in which banks compete with non-bank players. The internal governance of these businesses should be subject to the same activity-specific regulations that apply to non-bank players. Either exceptions within the regulatory framework or exclusions from the perimeter of prudential consolidation could be allowed.
- Plugging existing gaps in the regulation by **developing a regulatory and supervisory framework for new services**, such as virtual asset management, alternative finance (P2P) or financial service marketplaces. These rules should apply to both banks and non-bank players, the latter being authorised by narrowly defined (activity-specific) **FinTech licenses**.



Second, authorities should facilitate innovation for all players, under safe and even conditions, in case regulatory obstacles or uncertainties come to hinder the development of innovative solutions.

Regulatory sandboxes are a useful tool in this respect.

In order to improve the conditions that can lead to innovation, the regulatory sandboxes propose an space where regulators and market participants are better able to grasp each other's point of view, strengthening communication and increasing common understanding, and thus contributing to a significant reduction of bottlenecks. This experimental space involves a close control provided by the financial authorities with a regulatory relief for all participants, while ensuring protection for customers and for the economy as a whole. Its implementation adds significant value to regulators, consumers and entities, by allowing them to understand how the ecosystem works, the opportunities as well as the risks inherent in all the initiatives.

Last but not least, **cybersecurity** emerges as the main threat in this new environment. As the role of hyper connectivity grows in our daily lives, the security vulnerabilities are growing themselves – data theft, terrorism, intellectual property, corporate sabotage, denial of service, etc. The damages caused by cyber-attacks affect everyone, individuals, public sector and private sector, as recently happened with the cyberattack "Wanacry". In order to address the risks of cyber-attacks, both, the private and the public sector, are responsible for taking action in three different ways:

- **Education: awareness and training.** It is necessary to sensitize the population and companies that the risks of cybersecurity are there and it is impossible to protect ourselves 100%. In the field of training, people represent the first line of defense, so cybernetic talent must be continually updated. More than 70% of infractions exploit non-technical vulnerabilities, for example, attacks that trick users into revealing legitimate credentials.
- **Business scope:** to fight, companies must understand the risks they face and develop solid protection systems. A cyber-attack can bring you losses not only economically but also at the level of your reputation, your brand and your competitive position. They must have, in addition to a solid training of their employees with clear protocols of action before cyber-attacks.



- **Regulation, coordination and reporting.** Given that cyber risks are mostly cross-border, international cooperation between governments and the private sector is essential to effectively guarantee security and protection in cyberspace, while improving interoperability and management capacity. The European "one-stop-shop" mechanism is a big step in this direction.

Conclusion

Banks have always managed to make the most of technology to improve their efficiency and the service provided to their customers, but they now face a new wave of innovation with much wider implications for bank managers and public authorities.

The **new digital paradigm presents new risks** in terms of cyber security, consumer protection, operational continuity and fraud, among others, which are not fully covered by the traditional supervisory and regulatory approach. Hence there is a need for a renewed regulatory and supervisory framework that fully captures the potential of digital innovation and makes the financial system more resilient against future crises.

Every decision that public and private stakeholders make from now on must be approached with a great sense of responsibility, taking into account three key guiding principles. First, the **customer must be put at the center** of any initiatives with ambition to succeed. Second, as future developments in technology and the competitive landscape remain uncertain, we need to **pay special attention to the rise of new challenges**. And finally, **collaboration and communication** among all stakeholders is vital in order to make the most of digitisation in finance, while preserving financial stability and ensuring adequate consumer protection.