BANCA D'ITALIA

EUROSISTEMA

Mercati, infrastrutture, sistemi di pagamento

(Markets, Infrastructures, Payment Systems)

Technology providers in the payment sector: market and regulatory developments

by Emanuela Cerrato, Enrica Detto, Daniele Natalizi, Federico Semorile, Fabio Zuffranieri

March 2024

Number 47

BANCA D'ITALIA
EUROSISTEMA

Mercati, infrastrutture, sistemi di pagamento

(Markets, Infrastructures, Payment Systems)

Technology providers in the payment sector: market and regulatory developments

by Emanuela Cerrato, Enrica Detto, Daniele Natalizi, Federico Semorile, Fabio Zuffranieri

Number 47 – March 2024

The papers published in the 'Markets, Infrastructures, Payment Systems' series provide information and analysis on aspects regarding the institutional duties of the Bank of Italy in relation to the monitoring of financial markets and payment systems and the development and management of the corresponding infrastructures in order to foster a better understanding of these issues and stimulate discussion among institutions, economic actors and citizens.

The views expressed in the papers are those of the authors and do not necessarily reflect those of the Bank of Italy.

The series is available online at www.bancaditalia.it.

Printed copies can be requested from the Paolo Baffi Library: richieste.pubblicazioni@bancaditalia.it.

ISSN 2724-6418 (online)
ISSN 2724-640X (print)

Banca d'Italia
Via Nazionale, 91 - 00184 Rome - Italy
+39 06 47921

Designed and printing by the Printing and Publishing Division of the Bank of Italy

Technology providers in the payment sector: market and regulatory developments

by Emanuela Cerrato, Enrica Detto, Daniele Natalizi, Federico Semorile, Fabio Zuffranieri*

Abstract

Technology providers have taken on the crucial role in supporting the financial sector, enabling firms – even small ones – to become more efficient and keep pace with innovation. Yet, the interdependencies between such providers and financial entities may pose new systemic risks, deserving the attention of financial regulators and overseers. This paper presents the authorities' point of view, focusing on the payments sector; it demonstrates how numerous initiatives at international and national level have made a consistent and dynamic effort to create a regulatory and policy framework aimed at balancing security with innovation.

JEL Classification: E42, G32, G38, O33.

Keywords: payment system, market infrastructure, third parties, digital operational resilience, DORA, regulation, oversight.

* Bank of Italy, Market and Payment Systems Oversight Directorate.

CONTENTS

1. Introduction[1]

The reliable and efficient functioning of financial market infrastructures has always been essential to the development of advanced economies, safeguarding public trust in the currency, and facilitating the exchange of resources among economic operators as well as the allocation of risks among them. In this context, a key role is played by the payment system (hereafter also referred to as "ecosystem"), which encompasses all the components of the financial system that enable the safe and efficient execution of payments and securities transactions. Private-sector operators, such as consumers and businesses, public-sector operators, and the intermediaries themselves need access to effective and affordable means to send and receive payments. That is why exchange, clearing and settlement arrangements between financial operators are of the utmost importance.[2] However, the activities carried out in the payment ecosystem may pose risks, possibly causing serious disruption in the financial system, and affecting the real economy.

Thus, the smooth functioning of the payment ecosystem contributes to ensuring public trust in the economic and financial system. It relies on the efficiency, stability and security of the network of relationships among financial players, but also between them and their technology providers. The services and infrastructure provided by non-financial "third parties" have indeed become increasingly important in recent years due to the growing use of - and reliance on - advanced technological solutions to carry out financial transactions.

This paper sets out to analyze the main evolutionary trends in a scenario in which third parties have become increasingly important (section 2); it then presents the main regulatory initiatives at international, European and Italian level (sections 3, 4 and 5). Among such initiatives, the EU Regulation on "digital operational resilience for the financial sector" (Digital Operational Resilience Act – DORA) plays a prominent role, although not all payment ecosystem actors fall within its scope of application (section 6).

1.1 The term "Third party"

From an economic point of view, it appears easy to identify the underlying mechanisms for outsourcing services, as well as for using "third-party" providers more broadly. From a terminological point of view, however, the definition of "third party" can vary from regulation to regulation which is why we should clarify the subjective scope of this paper.

In this paper, the term "third party" refers to a non-financial provider of services and infrastructure supporting the business of financial players or the financial ecosystem as a whole, with a focus on the payments industry.

For example, it is used with this meaning in national secondary legislation and in the guidelines of the European Supervisory Authorities, in which the term "third party" generally refers to those providers that perform activities on behalf of the financial entities served (e.g. operators of market infrastructures including payment systems, banks, insurance companies). In outsourcing essential or important functions,[3] outsourcees – as the service buyers – are required

[1] The authors would like to thank Luca Arciero, Gino Giambelluca, Giuseppe Grande, Claudio Impenna and the anonymous referee for their helpful suggestions.

[2] Reference is made to the definitions set out in the Bank of Italy's Regulation of 9 November 2021. "Exchange" means the activity in which participants in the system exchange payment instructions, i.e. messages and orders for the transfer of funds, or the discharge of obligations via clearing. The subsequent "clearing" phase entails the conversion into a single credit or debit position – in accordance with the rules of the system – of the claims and debts of one or more participants vis-à-vis one or more other participants. "Settlement" discharges two or more participants' credit or debit positions.

[3] See, for example, the European Banking Authority's Guidelines on Outsourcing and Bank of Italy Circular No. 285.

to put in place a number of additional contractual and organizational safeguards, which supervisors monitor, thereby implementing an "indirect supervision" of third parties through the supervised financial entity. An example might be that of a bank using an external data center.

More recently, European Regulation No. 2554/2022 on Digital Operational Resilience for the Financial Sector (DORA) defines an information and communication technology service provider (ICT third-party provider) as that entity that delivers, on an ongoing basis, digital and data services to the financial entity, precisely through Information and Communication Technology (ICT) systems, including technical support and excluding traditional analogue telephone services.

This work does not cover the "third parties" introduced by European Directive No. 2366/2015 on Payment Services in the Internal Market (so-called Payment Services Directive 2 - PSD2), i.e. the operators specialized in the provision of services in the field of so-called "open banking",[4] which qualify as payment services in all respects.

2. Digital third-party providers in the payments system

2.1 The growing role of ICT third-party providers

The introduction of the Internet and especially the subsequent spread of Web 2.0, combined with the rapid development of other digital technologies such as mobile phones, have revolutionized the structure of the production system and the habits of individuals (Marchetti, 2022). Processes that previously required a high degree of human interaction have been automated; new products and services have also become commonly adopted due to users' growing familiarity with digital tools. Working through a computer, communicating with a smartphone, and initiating an online bank transfer are just a few examples of how people's lives have changed thanks to technology.

Digitalization has reshaped the banking and financial sector in the first place, facilitating the introduction of new business models, new competitors and new forms of competition through a gradual shift from physical to virtual channels.

The payment ecosystem has not been spared by such changes; rather, it has often been an area of early experimentation. In the past it was much more difficult to compete with traditional players, such as banks and the main credit or debit card payment circuits, where the way services were delivered and the resulting privileged relationship with customers were the main barriers to entry. Innovation has enabled users to choose among several alternative payment methods to cash, harmonized at the European level and geared toward instantaneous digital

[4] "Open banking" refers to a model for the use of financial data, related to customer payment accounts held with payment service providers, by "third-party" service providers, through the use of specific web-based technology interfaces to implement new services and applications. For a description of this sector of the industry, with reference to the Italian experience, see Pellitteri et al. (2023). PSD2 has introduced two new types of service providers, often referred to as Third-Party Providers (TPPs): Account Information Service Providers, which offer customers the possibility of accessing - through a single interface - consolidated information on one or more payment accounts even if held with different intermediaries; and Payment Initiation Service Providers, which allow a payment transaction to be performed against accounts held with other intermediaries. In addition, the Directive has introduced the possibility for a provider to issue payment cards linked to accounts held at another institution. The aforementioned services do not involve the direct holding of funds, but require the provider to be authorized to verify holdings on external accounts in a manner that is functional to the offering of its services.
Unlike the technology providers covered in this paper, whose operations are not subject to specific "statutory reservation of activity" regulatory regimes, PSD2 TPPs can only operate within the Union with a special license and offer services directly to end users.

interactions[5]. Today, BigTech[6] and fintech[7] start-ups can leverage network effects and underserved market niches to attract customers through the added value of their services by expanding or nimbly designing their offerings. A large part of BigTechs have already developed payment services such as digital purses (wallets) (e.g., Apple Pay, Google Pay, and Samsung Pay) and are leveraging partnerships with financial institutions to introduce new ones in banking and finance (EBA, 2021). Some of them already operate in the sector, for example through the presence within their group of companies registered or licensed by their respective authorities to provide payment services (Crisanto et al., 2021; Feyen et al., 2021).

The mechanisms that are "behind the scenes", i.e. the supporting infrastructure, have also undergone deep transformation: national payment systems are now deeply interconnected and pan-European solutions have been consolidated, with a web of direct and indirect relationships across borders. This has resulted in advantages in terms of both flexibility and efficiency in transaction execution and cost containment.

In this changed technological and industrial environment, the need and opportunity for financial players to use solutions offered by third parties has grown over time. Outsourced services, in particular, may involve some traditional functions, such as information-accounting systems, but more importantly, the development of innovative products, network connections, processing of commercial payments, etc.

The main economic reasons for financial system players to outsource services, especially in ICT, are identified in the literature (see, for example, McFarlan & Nolan, 1995; Currie et al., 2008; González et al., 2016; Könning et al, 2019) in the goals of (i) containing costs; (ii) focusing on the company's core business and strategic activities; (iii) acquiring know-how and professional skills not present internally; (iv) expanding the company's business offerings with innovative products; (v) activating new services in rapidly developing segments in a timely manner; and (vi) achieving a relatively lean capital structure.

The use of services provided by third parties especially facilitates the operations of smaller players who, with fewer resources available for technological investments, are able to contain costs and remain competitive in the market. This translates into potential positive externalities in the terms of increased market contestability.

In Italy, too, the change has been particularly pronounced, in a context in which banks historically ensured a widespread distribution of branches, characterized by close ties to the territory, and traditional promotion and distribution channels. The path towards digitalization has been undertaken precisely starting with payment services (Arnaudo et al., 2022)[8], where intermediaries have made increasing use of specialized players in order to evolve their offering. Examples of these trends can be identified in the development of "system" solutions for the services introduced by PSD2 (in this regard, see multi-operator platforms mentioned in section

[5] For example, the introduction, in the Single Euro Payments Area (SEPA), of common rules for making instant credit transfers, with immediate recognition of funds to the beneficiary, or the dematerialization of payment cards, which means that their issuance does not necessarily require a physical medium.

[6] The largest technology companies Amazon, Apple, Google, Meta (formerly Facebook) and Microsoft.

[7] The Financial Stability Board defines fintech as: "technologically enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services".

[8] Some studies (e.g. Coletti et al., 2022) confirm this trend, showing that the use of cash has been in constant decline from 2016, although it remains the most used means of payment; conversely, payments via electronic instruments have shown a continuous growth: between 2017 and 2021 the number of credit transfers grew - in Italy like in the Euro Area at a rate of 6%, while the number of card payments grew by 17% in Italy, more than the average in the Area (12%). The likelihood is that such instruments will be preferred by users in Europe in the near future.

5.2); on the same applies to the payment acceptance, where the use of third parties, the so-called Paytechs, is essential for the development of solutions for e-commerce or sophisticated POS (ECB, 2021b)[9].

2.2 Risks associated with the recourse to technological third-party providers and the role of regulation

Alongside the advantages just described, however, investments in technology and partnerships with third-party vendors have, over time, determined the manifestation of a strong dependence of financial system operators on such vendors and the need to adequately guard against related risks.

Financial players ever more rarely have the technical and economic capabilities to develop new solutions in-house, to adapt to market innovation or to re-internalize services. This situation results in heavy economic dependence on suppliers, with lock-in effects.

The increasing dependence on external suppliers has drawn the attention of regulators to the consequences that so-called "third-party" risks can cause both from a "micro" perspective at the level of the individual operator and from a "macro" perspective for the system as a whole.

The authorities' intervention is also justified by the fact that, from an operational point of view, outsourcing can be a bridge able to transfer risks between a regulated sector, that of the financial entity served, and an unregulated sector, that of the provider (BCBS, 2005) [10]. It becomes necessary to maintain a management framework and a right allocation of responsibility to avoid impairing supervision. In this sense, regulation has been aimed, on the one hand, at ensuring adequate risk management by entities that rely on third-party providers, also to avoid possible repercussions on end-users; and, on the other hand, at establishing new frameworks for the oversight of technology providers, which are not subject to financial sector regulation.

The use of outsourcing, and more specifically, the type of services outsourced and the economic conditions of the parties involved, require for the outsourcee to manage a number of risks[11]. Among the main ones, there are: 1) operational risk, where a problem occurring to a provider might affect the activity of the financial entity; 2) cyber risk, where the inadequacy of a provider's security policies might facilitate attacks on the financial entity, which could compromise its service availability, confidentiality and data integrity; and 3) reputational risk, where a provider's behavior might taint the reputation of the financial entity. Others include the risk of compliance with the regulatory framework and strategic risk, e.g. related to planning, programming and control choices.

From a systemic perspective, the use of third parties could pose risks to the overall stability of the system. For example, the risk of interconnectedness, which occurs when a third party provides services to a large number of financial entities. As a matter of fact, many interdependencies have developed over time between different payment systems and the

[9] The expansion of market offerings of increasingly innovative and digital payment methods and instruments correlates with the change in service level expectations and payment habits of consumers. For further discussion of the latter issue, see Coletti et al. (2022).

[10] Albeit in a less complex technological scenario, a set of guiding principles were published in 2005, given the growing relevance of outsourcing in finance.

[11] From the earliest cases of outsourcing IT services, Earl (1996) had identified as many as 11 generic risks arising from the process: (i) possibility of weakened management; (ii) staff without experience in the process; (iii) increased business uncertainty; (iv) obsolescence of in-house technological expertise; (v) endemic uncertainty; (vi) hidden costs; (vii) lack of experience economies; (viii) loss of innovative capability; (ix) difficulty of alignment among stakeholders; (x) indivisibility and rigidity of technology offerings to customers; and (xi) loss of IT strategic planning.

supporting technical infrastructure. In particular, specific providers, placed at critical nodes in the network, could become single points of failure and cause spill-over effects in the financial sector. Additionally, it should be considered that very often dependence on such "critical providers" is due to the peculiarity of the services offered. These include services that, like cloud computing, by their nature require a large dimensional scale and are spread across sectors. The above conditions actually amplify systemic riskiness, as the effects of any incident could propagate to all entities served, outside the financial sector too.

The interconnections between financial operators and supporting infrastructure just described may be physical and environmental, but with increasing digitalization they have taken on additional connotations in the cyberspace. Therefore, systemic players for the financial market are required to diversify the risk profile of their premises both geographically, in order to cope with natural disasters (e.g. a flood, an earthquake), and technologically, by preparing adequate resilience safeguards against cyber risk in order to avert a total or partial disruption of services (Giannetto and Fazio, 2022).

These are the elements on which the interventions of regulators have been based over the past 20 years, introducing oversight requirements and frameworks, coordinating initiatives among the various institutional levels to the extent possible. Regulation itself has been a real driver of change. Indeed, much of the recent technological development has been not only accompanied but also stimulated by significant regulatory development. One example is that of PSD2, which, in addition to regulating important innovations in the services offered to customers[12] and strengthening the payments chain through new and more stringent security measures, has prompted operators to develop technological solutions to support the evolution of the market at system level (see section 5.2). As evidence of the European legislator's continued focus on innovation in the payments industry, the European Commission carried out generalized and targeted consultations ahead of the PSD2 review, and in this context also asked questions about the role of technology providers in supporting this market[13]. In addition, the work at the European level on crypto-asset markets and the pilot regime for market infrastructures using Distributed Ledger Technology (DLT) are contributing to outline the necessary legal basis to support profound innovation, but also to oversee potential technological and third-party risks that solutions delivered by the industry may pose.

3. International principles and standards on third-party risk

Public intervention in the financial system, including the payment ecosystem, is justified due to the presence of market deficiencies - negative externalities, information asymmetries, and limitations in industry development - which prevent the achievement of a suitable equilibrium to ensure an optimal level of services.

[12] See in particular European Commission (2017), Revised rules for payment services in the EU: Summary of Directive (EU) 2015/2366 on EU-wide payment services.

[13] The following web pages can be consulted for further study:
https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Payment-services-review-of-EU-rules_en;
https://finance.ec.europa.eu/regulation-and-supervision/consultations/finance-2022-psd2-review_en.
On 28 June 2023 the European Commission published the proposals for review of the PSD2, under negotiation at the time of writing.

Since the early 2000s, in overseeing financial operators' risk management practices, regulators have developed specific requirements concerning outsourcing and engagement of external suppliers. Regulatory frameworks encompass principles, recommendations, and standards for effective management of risks by financial operators and efficient oversight by authorities.

3.1 Cooperation at global level

In the realm of payment systems, the initial mentions of outsourcing can be traced back to the Core Principles for Systemically Important Payment Systems (hereafter referred to as Core Principles) published in 2001 by the Committee on Payment and Settlement Systems (CPSS)[14] of the Bank for International Settlements (BIS). The Core Principles urged payment system operators to establish redundant communication lines and infrastructure, as well as to negotiate appropriate Service Level Agreements (SLAs) with telecommunications service providers.

A further advancement in the framework for third-party oversight occurred in 2012, when the CPSS of the BIS, in collaboration with the Technical Committee of the International Organization of Securities Commissions (IOSCO), updated the risk management framework for financial system infrastructures (including the Core Principles[15]). This update resulted in the publication of a unified set of principles known as the Principles for Financial Market Infrastructures (PFMI). Recognizing the growing significance of third parties in providing technology support to the financial system, the PFMI incorporate numerous references to external service providers. These references address not only operational risk but also other aspects where third parties can play an 'active' or 'passive' role, introducing or facing risks in their relationships with a Financial Market Infrastructure (FMI)[16]. Additionally, the PFMI are accompanied by a specific annex (Annex F) containing Oversight Expectations applicable to critical service providers. These expectations, largely derived from the High-Level Expectations for the oversight of SWIFT (Society for Worldwide Interbank Financial Telecommunication) (see paragraph 3.2), are directly targeted at critical providers. The new expectations encompass risk identification and management, robust information security management, reliability and resilience, effective technology planning, and secure communications with users.

The PFMI and their annexes constitute a principle-based regulatory framework that has demonstrated its ability to remain relevant and adaptable over time. It serves as a guiding reference for both authorities and operators. Complemented by subsequent reference documents and interpreted in an evolving manner, the PFMI form the basis for initiatives aimed at mitigating risks arising from the application of new technologies in the financial domain, including those supporting crypto-assets. Importantly, these efforts aim to harness the potential of these

[14] Now Committee on Payments and Market Infrastructures (CPMI).

[15] The CPSS and *the Technical Committee of the International Organization of Securities Commissions (IOSCO) developed* specific sets of recommendations for the different infrastructures, among which the *Recommendations for securities settlement systems* and the *Recommendations for central counterparties.*

[16] The PFMI define a financial market infrastructure as a multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions. The definition encompasses payment systems, securities settlement systems, central securities depositories, central counterparties and repositories of trade data (so-*called trade repositories).*

technologies for the benefit of the ecosystem, its constituents, and the citizens as end-users, while ensuring responsible risk management[17].

3.2 SWIFT: a case study

While not directly aimed at third parties, but rather at the payment systems they serve[18], the *Core Principles* have laid the foundation for the establishment of a framework of requirements applicable to SWIFT. As one of the leading providers of messaging and network services in the international financial system, SWIFT connects operators for cross-border payments and securities exchange worldwide[19].

Central banks monitor SWIFT's compliance with the requirements, based on what has become one of the earliest models of international cooperative oversight, necessary due to its 'borderless' operations. Since 2004, SWIFT has been subject to cooperative oversight by the central banks of the G10 countries, with the National Bank of Belgium (NBB), the central bank of the country where SWIFT is headquartered, acting as the Lead Overseer. The NBB entered into a protocol with SWIFT, which regulates the objectives, scope, and conduct of the oversight activities. This was followed by the establishment of bilateral Memoranda of Understanding between the NBB and the central banks of the G10 countries, delineating their respective areas of responsibility and participation in these efforts[20].

The SWIFT case is particularly relevant, as the oversight framework developed by the cooperative oversight group led to the formulation of five specific principles for operational risk management: the High-Level Expectations for the oversight of SWIFT, previously mentioned in paragraph 3.1. The expectations laid the foundation for Annex F of the PFMI, which currently constitutes the set of requirements to which every critical service provider should adhere. At the time of drafting, each 'expectation' referred to an objective that authorities intended for SWIFT to achieve in terms of resilience and operational risk management. The qualification as 'high level' aimed to grant SWIFT a degree of flexibility in choosing the methods to achieve the objectives, as well as in adopting risk management processes and reporting mechanisms towards authorities. This was not about merely adhering to industry best practices, because given SWIFT's global significance, the expectation was that the company would exceed such standards.

3.3 The G7 "fundamental elements" on third-party cyber risk

---

[17] See CPMI-IOSCO (2016), *Guidance on cyber resilience for financial market infrastructures*; CPMI-IOSCO (2022), *Application of the Principles for Financial Market Infrastructures to stablecoin arrangements*.

[18] The majority of the Core Principles (6 out of 10) pertained to financial risk profiles typical of payment systems and their participants, not directly related to third parties. Only a few of the Core Principles, when appropriately interpreted, appeared to be applicable to third parties as well: having a robust legal foundation for their operations, establishing non-discriminatory access criteria for their services, and having adequate governance structures. Out of the ten Core Principles, only one would have been readily applicable to third-party technology service providers, i.e. the principle concerning operational risk.

[19] SWIFT operates in 28 countries and employs over 2,800 personnel. The SWIFT infrastructure links approximately 11,000 financial operators (comprising banks, depositories, investment institutions, central banks, market infrastructures, and corporate clients) spread across more than 200 countries. In the year 2022, these entities exchanged an average of 44.8 million messages per day.

[20] Oversight activities are carried out through the efforts of four groups: 1) the Cooperative Oversight Group, composed of central banks from the G10, which formulates oversight strategies and policies; 2) the Executive Group, comprising representatives from NBB, ECB, Federal Reserve Board, Bank of Japan, and Bank of England, acting as representatives of the Oversight Group in discussions and communications with the SWIFT Board; 3) the Technical Group, responsible for deliberating on technical aspects before presenting them to the Oversight Group; 4) the Oversight Forum, facilitating discussions on SWIFT's global strategies and the technological evolution of service providers for the financial sector beyond the G10. The oversight activities cover governance frameworks, structures, processes, procedures, and control systems, with a particular emphasis on operational risk and service continuity.

The growing interconnection between technology and finance increases operators' exposure to cyber risk. Not by chance, the finance ministers and central bank governors of the G7 have been devoting growing attention to the possible risks to the financial sector arising from third-party services. In October 2022, the latest version of "The G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector" was published, as the result of the continuous updating of principles firstly issued in 2016.

The document contains a set of key elements for managing third-party cyber risk, taking into account the increasing outsourcing of ICT services and the new threats to the financial supply chain. The fundamental elements are high-level principles that financial authorities in different jurisdictions may refer to in their policy, regulatory and supervisory activities, in seven areas: 1. governance; 2. risk management; 3. incident response; 4. contingency planning and exit strategies; 5. monitoring of potential systemic risk; 6. cross-sector coordination; and 7. specificity of third parties in the financial sector.

4. The European oversight framework

Article 3 of the Statute of the European System of Central Banks and Article 127 of the Treaty on the Functioning of the European Union entrust European central banks with the task of promoting the smooth functioning of payments system. In the euro area this objective has been transposed into standards, guidelines and regulations that set requirements for the oversight of systems and relevant participants. The requirements, as part of the Eurosystem Oversight Policy Framework (ECB 2016), are accompanied with common methodologies aimed at harmonized implementation and level playing field among overseen entities in different across jurisdictions.

The oversight perimeter - which varies in breadth and depth over time, in an evolving scenario - includes the so-called Critical Service Providers (CSPs), i.e. providers of technical services and infrastructure that play a key role in the payment ecosystem.

4.1 The identification of Critical Service Providers

The Eurosystem oversees the CSPs that serve the FMIs under its remit, in line with the policy adopted by the Governing Council of the European Central Bank in 2017[21]. In the broader context the aforementioned Eurosystem Oversight Policy Framework, the policy draws inspiration from established international practice, in particular, based on Annex F of the PFMIs.

The *policy* defines a CSP as "*a service provider that has a direct contractual arrangement with an FMI to provide, on a continuous basis, services to that FMI (and potentially its participants) which are essential for ensuring information confidentiality and integrity and service availability, as well as the smooth functioning of its core operations",* where essential services comprise *"data centres, financial messaging/network services, payment processing services, settlement functionality, or other business applications related to payment/clearing/settlement services*"[22].

[21] *Eurosystem policy for the identification and oversight of critical service providers of financial market infrastructures*.

[22] See ECB (2017) Eurosystem oversight report 2016 and ECB (2021a) Eurosystem oversight report 2020.

In order to actually identify CPs, the Eurosystem periodically surveys the euro area FMIs. The survey covers the payment ecosystem in a broader sense, encompassing systemically important payment systems, retail payment systems, card schemes, and the TARGET2-Securities settlement platform[23].

Providers identified within the survey, are successively evaluated based on specific criteria to determine their criticality to FMIs in the relevant ecosystem, and ranked according to the type of services they offer. Finally, the most appropriate surveillance approach is chosen (see Section 4.2).

The policy highlights the sensibility of European authorities on third parties that provide services and technological solutions to financial operators of payment ecosystem, taking into account a significant dependence of FMIs from external providers of digital resources and interdependency. At the same time, the cross-sectorial and borderless nature of digital technologies requires a strong cooperation among European authorities.

4.2 Oversight approach

CSPs are subject to direct or indirect oversight, or to monitoring, depending on their specific features and those of the ecosystem they support. CSPs include entities established both within and outside the European Union, which are active in specific segments or provide a plurality of services.

The Eurosystem defines the most appropriate oversight approach in three steps:

i. identification of the technical service providers supporting the FMIs that fall under its oversight mandate;
ii. identification of the subset of technical service providers to be considered "critical", based on high-level criteria such as the importance of the provider to the entity it serves and to the ecosystem at large, as well as the absence of alternative providers;
iii. adoption of the most appropriate approach and the most effective way of conducting oversight, taking into account numerous factors, among which the powers that may be exercised in the national jurisdictions, which may range from moral suasion to the enforcement of binding rules.[24]

Where the CSP offers services to several FMIs, it will typically be subject to direct oversight; the latter may take on a national or cooperative connotation, depending on the extent to which the CSP is active at 'cross-border level.

A CSP may be subject to indirect oversight through requirements imposed on the overseen entity it serves. In line with common principles and practice in finance, the FMI remains fully responsible for outsourced activities.

Where the CSP would not need to be directly overseen, authorities may opt for monitoring, especially in case the provider's characteristics would require constant attention to

[23] The *policy* and the connected survey have a broad scope, including card schemes and the T2S platform, although they do not meet the definition of FMI. Lastly, the *Eurosystem oversight framework for electronic payment instruments, schemes and arrangements* (so-called PISA Framework) puts forward the expectation that governance authorities of schemes and "*arrangements*" participate in the survey, thus likely further enlarging the coverage of the payment ecosystem in this exercise. The Framework defines an *arrangement* as *"a set of operational functionalities which support the end users of multiple payment service providers in the use of electronic payment instruments. The arrangement is managed by a governance body which, inter alia, issues the relevant rules or terms and conditions"*.

[24] For example, the Consolidated Law on Banking expressly provides the Bank of Italy with oversight powers over providers of technological or network infrastructure (see section 5.2).

the evolution of its operations (e.g. in terms of growth potential or high relevance to specific FMIs).

4.3 Oversight requirements and process

Among the oversight tools, a prominent role is played by the aforementioned Annex F of the PFMIs (see section 3.1), which acts as a guide for the CSP and the authorities; it defines the methodology for verifying compliance with the expectations contained in the Annex, based on a set of key questions for each of the five risk profiles.

Typically, upon request of the oversight authority, channeled through the overseen entity served, the CSP performs a self-assessment exercise against the expectations. As a matter of fact, Annex F was created as a tool for indirect oversight, but it is a fundamental reference for direct oversight as well. Specifically, in the case of indirect oversight, the overseer analyzes: i) the CSP's self-assessment, provided to the FMI, against the expectations contained in Annex F; ii) the outsourcing relationship between the FMI and the CSP in terms of overall contractual robustness and specific provisions (service levels agreements, performance indicators, possibility to perform audits and inspections at the CSP's premises).

5. The Italian oversight framework

5.1 Legal foundation

With Article 146 of Legislative Decree No. 385/1993 (the so-called Consolidated Law on Banking - CLB), the Italian legislator entrusted the Bank of Italy with the objective of ensuring the smooth operation of the payment system[25] in terms of reliability, efficiency and users protection, granting it regulatory, informational, inspection and inhibitory powers for those purposes.

The same article identifies the categories of entities towards which the Bank of Italy can exercise its oversight powers: technological or network infrastructure providers are included.

5.2 Implementing regulations issued by the Bank of Italy

In 2021, the Bank of Italy issued the "Regulation concerning the oversight of payment systems and the supporting technological or network infrastructures, which innovated the pre-existing secondary oversight legislation by extending - in accordance with Article 146 of the CLB - its scope of application to operators of all - including wholesale - payment systems and providers of supporting technological or network infrastructure.

The broadening of the scope intends to respond to both the progressively blurred distinction between wholesale and retail payments has become[26], in terms of speed of execution[27]

[25] There are significant links between the smooth operation of payment systems and other public interests; the efficiency and reliability of payment systems contribute to the proper transmission of monetary policy and to financial stability.

[26] E.g. the distinction between "wholesale" and "retail" is not relevant for the purpose of assessing the systemic importance of a payment system under European Central Bank Regulation No. 715/2014 on oversight requirements for systemically important payment systems (as amended and supplemented).

[27] Instant payments introduced a few years ago make it possible, even in the retail environment, to immediately execute transfers of funds between accounts, once possible only at the interbank level using real time gross settlement systems (RTGS).

and amounts processed, and the growing role of technological or network infrastructures in the financial industry, which requires stronger safeguards against the risks related to the use of external providers by market operators.

In reviewing the oversight Regulation, particular attention was paid to the role of technology providers. As matter of fact, as already argued, technological advances and the diversification of business models have made the payments chain more complex, and have increased the number of players involved; this has called for more detailed regulation, not only of transactions exchange, clearing and settlement activities[28], but also of supporting technical activities, on which the reliability and efficiency of the ecosystem as a whole increasingly depend.

The Regulation of 2021 hence devotes a section to technology providers, listing the main technical services that support the payment system, from the more ""traditional"" messaging and network services, to multi-party platforms[29] that enable open banking functionalities (Table 1).

Table 1: Examples of technological or network infrastructure subject to oversight in Italy (1)

- messaging and network services
- business services and/or applications for processing and exchanging financial and information flows, clearing and/or settlement of payment transactions between payment service providers and/or between payment service providers and customers
- services for retaining and processing sensitive payment data, including user security credentials and routing payment data
- services for processing payment transactions (2)
- multi-party interface services to enable third-party access to accounts (3)

(1) See Article 19 of the Bank of Italy "Regulation concerning the oversight of payment systems and the supporting technological or network infrastructures" of November 9, 2021.
(2) Services referred to in Article 2, paragraph 1, number 28 of Regulation (EU) No. 2015/751 on interchange fees on card-based payment transactions.
(3) Pursuant to Commission Delegated Regulation (EU) No. 2018/389 of November 27, 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong client authentication and common and secure open communication standards.

Pursuant to the Regulation, providers are required to notify their start of operations, with no less than three months' notice. The notification is also instrumental to the Bank of Italy's broader monitoring of the market and its operators.

[28] Article 1 of the Bank of Italy Regulation of 9 November 2021 defines: 'exchange' *as the activity in which participants in the system exchange payment instructions, i.e. messages and orders for the transfer of funds, or the discharge of obligations via clearing; the operator may directly draw up rules for the exchange activity or make reference to rules defined by others*; 'clearing' as *the conversion into a single credit or debit position – in accordance with the rules of the system – of the claims and debts of one or more participants vis-à-vis one or more other participants pursuant to the exchange of payment instructions*; 'settlement' *as the discharge of two or more participants' credit or debit positions*.

[29] I.e. technical infrastructure for the provision of payment services through the use of application programming interfaces (APIs), standards and IT protocols enabling communication and integration between different applications for the exchange of information flows between multiple links in a renewed payment chain. APIs allow TPPs to connect to a plurality of intermediaries through a single point of access. For further details, see Pellitteri et al. (2023).

Applying the proportionality principle, the Bank of Italy identifies those providers that are critical to the orderly functioning of the Italian payment system, and thus subject to specific disclosure obligations and risk management requirements.[30]

The provider's criticality is primarily evaluated on the basis of certain criteria set out in the Regulation:

i. provision of infrastructure or technical services essential to the confidentiality, integrity and availability of the data processed for a significant share of the Italian market;
ii. importance for the Italian market of the payment systems served; and/or
iii. absence of alternative providers for the users served.

The evaluation is carried out as part of an administrative proceeding, which is conducted as described in the "Guide for controls" annexed to the Regulation. The Guide, together with another annex containing "Measures on business continuity", complements the national secondary legislation. With a view to maximizing the transparency of the Bank of Italy's actions, the annexes to the Regulation help the operators and providers to perform their oversight obligations: the Guide provides methodological support; the second annex provides a framework for the business continuity measures to be adopted.'' Implementing Article 146 of the CLB, the Regulation provides further legal certainty with respect to the Bank of Italy's oversight of the technology providers and strengthens third-party risk protection in the sector.

This approach ensures alignment with supranational practice, safeguarding against the risks posed by critical actors in the national market, while avoiding overlap of competences or duplication of controls.

6. The Digital Operational Resilience Act

The digital finance package, published by the European Commission in September 2020, comprises a proposal for harmonized primary law on the digital operational resilience of the financial sector, taking the form of an EU Regulation (so-called Digital Operational Resilience Act – DORA)[31]. The Regulation was published on the EU Official Journal on 27 December 2022, came into force after 20 days and will be applied after two years. Amongst others, it addresses third-party risk from two angles: indirectly, setting out requirements for financial entities in their relationships with technology providers, and directly, establishing a new European framework for the oversight of those providers considered critical.

A premise on the scope of application of DORA is of help to outline the relevant provisions of third-party risk.

[30] In particular, the following articles of the Regulation: Article 4 on organization, Article 5 on the effectiveness of controls, Article 6 on outsourcing, Article 9 on business risk, Article 10 on legal risk and Article 11 on operational risks.

[31] As regards the type of the legal act, a Regulation was chosen to attain utmost harmonization of the provisions on digital operational resilience in the financial sector. DORA will hence be directly applicable in the EU Member States, with EEA relevance. Specific provision of the Regulation will be further detailed through "level 2" measures (Guidelines, Regulatory Technical Standards and Implementing Technical Standards).
The negotiations started during the German Presidency of the EU Council in 2020. After the agreement at Council level, the trilogue began in H1 2022 (European Commission, European Parliament, EU Council). The final text was published under Czech Presidency (EU Regulation 2022/2554). Since the publication of the proposal for a legal act in September 2020, national delegations discussed the many topics addressed by DORA. The topics were at the same time debated among market operators, and between such operators and public authorities. The Bank of Italy contributed to the works in several fora: it supported the Italian delegation participating in the negotiations at Council level; it promoted the exchange of views with the market; it participated in the decision-making process resulting in the ECB's opinion on the proposal for a Regulation.

As regards the subject matter of DORA, i.e. "digital operational resilience"[32], it is worth analyzing the use of the term "resilience" rather than the more traditional reference to "security", as well as its qualification as "operational" and "digital". The difference between security and resilience is relatively nuanced, with partial overlap. The former can generically be intended as safeguard against risks; the latter includes security and sets it into the broader context of identification, detection, protection, management, response and recovery from risks and malicious events. The concept of resilience is often associated to cyber risk; it is qualified as "operational" since it is instrumental to the regular operation of the entities and the market sector in question, and as "digital" in light of the strong use of ICT resources. The pursuit of digital operational resilience hence marks a turning point compared to that of business continuity, enlarging the exclusive focus on uninterrupted service availability to encompass the integrity and confidentiality of the underlying data. Resilience is upgraded to a strategic goal of each financial entity, and as such is integrated into the governance and internal controls framework, aimed at an effective comprehensive management of ICT risks. And, indeed, third-party risk management ever more contributes to digital operational resilience.

As regards the entities in scope, as mentioned above, DORA covers the "financial sector". The new provisions are addressed to 20 typologies of financial entity, aiming to overcome the fragmentation that has existed so far, with heterogeneous regulations across sub-sectors, and, sometimes, with national specificities. Harmonization is particularly relevant to entities in more countries and sub-sectors. DORA also introduces a European oversight framework for critical service providers, thus going beyond the financial sector.

Operators of payment systems and entities involved in payment-processing activities (e.g. card schemes) are subject to DORA. That choice, as the Commission highlighted in the first phases of the work[33] and most recently in the report to the Parliament and the Council on the PSD2 review[34], takes into account the specificities of the relevant regulatory and oversight framework, including the central banks' competences in the field of payment systems (as per art. 127 of the Treaty), which already result in a robust system of requirements and controls on digital operational resilience. The opportunity to enlarge the scope of application of DORA will be reexamined in the context of the review of the Regulation.

Among the aspects that were discussed the most during the negotiations, it is worth highlighting the implications of the Regulation on the existing competences of national and European authorities, with specific regard to the oversight of critical ICT service providers, and the interplay with other European legislative proposals on ICT and physical security in vital sectors of societal and economic life.

6.1 Interplay with other regulations

[32] Art. 3 of the Regulation defines "digital operational resilience" as: "*the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions*".

[33] See the *Explanatory Memorandum* accompanying the European Commission's proposal of 24 September 2020.

[34] See review clause contained in art. 58 of DORA, according to which the Commission should report to the Parliament and the Council on the opportunity to include operators of payment systems and entities involved in payment-processing activities in the scope of application of DORA; Report from the Commission to the European Parliament, the Council, the European Central Bank and the European Economic and Social Committee on the review of Directive 2015/2366/EU of the European Parliament and of the Council on payment services in the internal market of 28 June 2023.

As regards the third-party risk management requirements addressed to financial entities, DORA also provides for the possibility to use standard contractual clauses in outsourcing arrangements. Third-party risk management in the context of outsourcing is already highly regulated in the financial sector. Suffice it to think of the ESA guidelines on outsourcing, including those specifically targeting cloud services[35]. DORA "upgrades" the relevant requirements from secondary to primary law in Europe.

Moreover, the topic of digital operational resilience is intertwined with that of network and information systems security, which is addressed – at cross-sector level – by the EU Directive n. 2016/1148 (so-called NIS Directive), now repealed by n. 2022/2555 (NIS2). DORA is *lex specialis* vis-à-vis the NIS/NIS2 Directive for the financial sector. This entails that – in case of overlap – NIS provisions are disapplied in favor of DORA for the financial sector; there remains the need to bridge the two ecosystems of authorities, especially in terms of adequacy and timeliness of information flows.

The NIS applies to three categories of financial entity (banks, trading venues, central counterparties), requiring that they adopt specific security measures, and notify relevant incidents, if identified as operators essential to maintain fundamental societal or economic activities It is aims at minimum harmonization, and does not affect the measures that Member States may have adopted to safeguard national security. In Italy, the Directive was transposed though Legislative decree n. 65 of 18 May 2018, amended by Decree-law n. 82 of 14 June 2021, converted into Law n. 109 of 4 August 2021, which defined the national cybersecurity architecture and created the National Cybersecurity Agency.[36]

Finally, the topics of digital operational resilience and of network and information systems security touch upon national security, which remains the remit of each Member State's legislator. In Italy, in line with a trend prevailing in several countries, the legislator is sensitive to cyber security, which has formed the subject of many regulatory interventions.

Decree-law n. 105 of 21 September 2019, converted into Law n. 133 of 18 November 2019, laid the foundation to design the national cybersecurity perimeter, comprising public- and private-sector entities established in Italian territory, and depended upon for essential State functions, or services essential to maintain civil, societal, or economic activities, which are in turn fundamental to the Sate's interests and the (partial) failure or interruption or improper use of which may harm national security. Such entities are required – amongst others –to adopt specific security measures, and notify relevant incidents. The law considers the case of entities that are both included in the perimeter and subject to NIS provisions, so as to avoid duplications and adequately coordinate the two sets of provisions. The National Cyber Agency has specific competence to apply the legislation on the national cybersecurity perimeter.

[35] See EBA (2019), Final Report on EBA Guidelines on outsourcing arrangements, EBA/GL/2019/02; ESMA (2020), Final Report - Guidelines on outsourcing to cloud service providers, ESMA50-157-2403; EIOPA (2020), Guidelines on outsourcing to cloud service providers, EIOPA-BoS-20-002.

[36] The Agency has been appointed as the Italian NIS competent authority, with the support of the Ministries in the specific sectors. Further reviews may stem from the repeal of the NIS Directive the transposition of the NIS2 Directive into national law; in any case, the minimum harmonization nature, and the categories of financial entities in scope are confirmed.

6.2 The critical ICT provider oversight framework

DORA gives new oversight tasks and powers to European and national authorities, in a multi-layer governance structure. The creation of a third-party provider oversight framework is not new as such. It is new in that it is created at European level, through harmonized primary law, for the financial system as a whole. DORA itself acknowledges pre-existing oversight frameworks when excluding from its scope of application those ICT service providers that are subject to oversight based on article 127 of Treaty, in pursuit of the smooth functioning of payment systems. Additionally, DORA excepts national frameworks for the oversight of those providers that may be relevant at domestic level. As far as Italy is concerned, the oversight framework resulting from the Regulation issued by the Bank of Italy on 9 November 2021 (see section 5.2) will coexist with that created by the EU Regulation, since the former covers providers deemed critical for the national financial marketplace, and is to be set into the context of the central bank's competences stemming from the Treaty and from the Italian Consolidated Law on Banking. Finally, DORA is linked to the NIS2 ecosystem as regards digital service providers, which remain subject to both pieces of legislation.

The European Supervisory Authorities (ESAs) play a key role in the new oversight framework: DORA gives them tasks and powers to oversee critical providers. It is the first such legal act to entrust the ESAs with oversight tasks, while they were created to strengthen the stability and efficiency of the financial system in the EU, in particular issuing guidelines.

As for the institutional architecture, one of the ESAs[37] is appointed as the Lead Overseer, depending on the sub-sector (banking, securities or insurance) that relies the most upon the overseen provider[38]. The oversight activity will be performed within a multi-layer organization under the lead of ESAs: i) the Joint Committee, which designates critical third parties, appoints one of the ESAs as the Lead Overseer competent for each third party, provides guidance and promotes coordination; ii) the Oversight Forum[39] provides operational support to the Committee, preparing reports and joint positions, and developing collective assessments; iii) the Joint Oversight Network, allowing additional operational coordination across Lead Overseers.

Lead Overseers are endowed with specific powers, such as: i) ask for the information and documentation necessary to continuously monitor the critical provider's operations; ii) conduct "general investigation" and on-site inspections[40]; iii) issue recommendations; iv) impose pecuniary sanctions.

The governance assigns different roles to ESAs on the one hand, which are responsible for the oversight of the third parties, and the national competent authorities on the other, which are responsible for the supervision of the financial entities served. The latter are also in charge of the supervisory feedback, i.e. the task to inform supervised financial entities of the risks that the critical third party may pose and of the recommendations that the Lead Overseer may have addressed to it; the authorities may request that the financial entities adopt specific measures as

[37] The European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) or the European Insurance and Occupational Pensions Authority (EIOPA).

[38] In detail, the appointed Lead Overseer for each ICT third-party provider is the ESA responsible for the financial entities which together account for the majority of total assets, out of the assets of all the financial entities using the provider's services, summing up the values in their balance sheets.

[39] The ECB and other relevant authorities also participate.

[40] In conducting such activities, the Lead Overseers are supported by Joint examination teams, i.e. groups created for each critical provider, and comprising staff from national authorities.

deemed opportune. After evaluating such measures and in the event of the critical provider's continued non-compliance with the recommendations, national authorities may adopt such measures of last resort vis-à-vis the financial entities as the request to temporarily suspend the use of the service and, ultimately, to terminate the contract.

The Joint Committee identifies the critical providers according to four non-alternative criteria, concerning: a) systemic impact on the stability, continuity or quality of financial services in the event of large scale operational failure faced by the provider; b) systemic relevance of the entities served; c) financial entities' reliance on the third party to perform their critical or important functions; d) the degree of provider's substitutability, taking into account the (lack of) real competitors and the feasibility of migrating data and workloads to one of them. Following a call for advice from the Commission to the ESAs, technical work has been undertaken to articulate such criteria through operational rules to be used for the actual identification of critical third parties.

Based on the above criteria, the category might include the so-called BigTechs that offer cloud computing services to financial entities, given the relative concentration and importance for the market. The BigTechs would fall within the scope of a financial oversight framework[41] for the first time in Europe. More traditional providers, like messaging or network service providers, may equally fall within the scope.

Finally, there are exceptions for specific kinds of provider, for example: i) financial entities providing ICT services to other financial entities; ii) intra-group service providers, i.e. providing predominantly ICT services to financial entities within their group; iii) third parties providing ICT services solely in one Member State to financial entities that are not active at cross-border level. Finally, as mentioned above, the new rules do not apply to providers already under the remit of Eurosystem oversight as per Article 127(2) of the Treaty.

7. Conclusions

The crucial importance of technology to the financial industry and the payment ecosystem is a hallmark of modern economies.

Against this background, outsourcing strategies and a growing use of third-parties services have enabled companies, especially smaller ones with limited resources, to keep pace with the innovation that has characterized the industry over the past 20 years. This, however, has exacerbated a range of risks (operational, cyber, concentration, reputational, strategic risk) which, when services and functions are transferred from regulated sectors to third parties outside such perimeter, might fly under the authorities' radar.

Along with the emergence of increasingly innovative and digitalized products in the financial and payment system, this explains the growing attention paid and the efforts made by regulators, at both international and national level.

The initiatives of authorities, standard setters and regulators analyzed in this paper can be grouped into two main areas: i) interventions aimed at financial entities to manage third-party risk; ii) new frameworks for the oversight of third parties.

[41] The BigTechs fall within the scope of a broader set of European pieces of legislation, among which the so-called Digital Markets Act, considering their role as "gatekeepers" or facilitators for the access to several online services. the interplay between the different oversight and competition requirements is of interest to the authorities that will apply the new legal acts.

The Principles for Financial Market Infrastructures (PFMI) remain the international benchmark, and regulators' actions, especially if we focus on Europe and Italy, have strived to guarantee utmost consistency with international best practices.

DORA aims to harmonize the actions to improve the resilience of the financial sector, considering its high reliance on ICT resources, and it assigns a new role to the European Supervisory Authorities (EBA, EIOPA, ESMA) in the critical third-party oversight framework. At present, not all operators in the payment ecosystem fall within the scope of application of DORA; in any event, the resilience of that ecosystem is ensured by consolidated sectoral regulation.

Third-party risk is relevant to the financial sector as a whole, and is all the more relevant considering the web of interdependencies between financial and non-financial operators, which cross national borders and remodel consumers' economic and social behavior.

Mitigating this kind of risk helps to increase the operational resilience of the sector and its operators, with the ultimate goal of protecting the end users of financial services. It also strengthens public trust in the authorities, who have always pursued an optimal balance between security and innovation.

References

Arnaudo D., Del Prete S., Demma C., Manile M., Orame A., Pagnini M., Rossi C., Rossi P., & Soggia G. (2022), "The digital transformation in the Italian banking sector", *Banca d'Italia - Questioni di Economia e Finanza*, No. 682, April 2022.

BCBS, Basel Committee on Banking Supervision (2005), Outsourcing in Financial Services, February 2005.

Coletti G., Di Iorio A., Pimpini E. & Rocco G. (2022), "Report on the payment attitudes of consumers in Italy: results from ECB surveys", *Banca d'Italia - Mercati, infrastrutture, sistemi di pagamento*, No. 22, March 2022.

CPMI-IOSCO, Committee on Payments and Market Infrastructures - International Organization of Securities Commissions (2012), CPMI-IOSCO Principles for Financial Market Infrastructures, April 2012.

CPMI-IOSCO, Committee on Payments and Market Infrastructures - International Organization of Securities Commissions (2016), Guidance on cyber resilience for financial market infrastructures, June 2016.

CPMI-IOSCO, Committee on Payments and Market Infrastructures - International Organization of Securities Commissions (2022), Application of the Principles for Financial Market Infrastructures to stablecoin arrangements, July 2022.

Crisanto J. C., Ehrentraud J., & and Fabian M. (2021), Big techs in finance: regulatory approaches and policy options, *BIS, Bank for International Settlements – FSI Briefs*, No. 12, March 2021.

Currie W. L., Michell V., & Abanishe O. (2008). Knowledge process outsourcing in financial services: The vendor perspective. *European Management Journal*, 26(2), 94-104.

Earl M. J. (1996). The risks of outsourcing IT. *MIT Sloan Management Review*.

EBA, European Banking Authority (2019), Final Report on EBA Guidelines on outsourcing arrangements, EBA/GL/2019/02, February 2019.

EBA, European Banking Authority (2021), Report on the use of digital platforms in the EU banking and payments sector (EBA/REP/2021/26), September 2021.

EC, European Commission (2017), Revised rules for payment services in the EU: Summary of Directive (EU) 2015/2366 on EU-wide payment services, December 2017.

ECB, European Central Bank (2016), Eurosystem oversight policy framework, July 2016.

ECB, European Central Bank (2017), Eurosystem oversight report 2016, November 2017.

ECB, European Central Bank (2021a), Eurosystem oversight report 2020, April 2021.

ECB, European Central Bank (2021b), Payments and market infrastructure two decades after the start of the European Central Bank, July 2021.

ECB, European Central Bank (2022), Eurosystem oversight framework for electronic payment instruments, schemes and arrangements, November 2021.

EIOPA, European Insurance and Occupational Pensions Authority (2020), Guidelines on outsourcing to cloud service providers (EIOPA-BoS-20-002), February 2020.

ESMA, European Securities and Markets Authority (2020), Final Report - Guidelines on outsourcing to cloud service providers (ESMA50-157-2403), December 2020.

Feyen E., Frost J., Gambacorta L., Natarajan H., and Saal M. (2021), Fintech and the digital transformation of financial services: implications for market structure and public policy, *BIS, Bank for International Settlements - BIS Papers*, No. 117, July 2021.

Giannetto B. & Fazio A. (2022), "Cyber resilience per la continuità di servizio del sistema finanziario", Banca d'Italia - *Mercati, infrastrutture, sistemi di pagamento*, No. 18, March 2022.

González R., Gascó J., & Llopis J. (2016). Information systems outsourcing reasons and risks: review and evolution. *Journal of Global Information Technology Management*, 19(4), 223-249.

G7 (2022), Fundamental elements for third party cyber risk management in the financial sector, October 2022.

Könning M., Westner M., & Strahringer S. (2019). A systematic review of recent developments in IT outsourcing research. *Information Systems Management*, *36*(1), 78-96.

Marchetti S. (2022), "Web3, Blocksplained", *Banca d'Italia - Questioni di Economia e Finanza*, No. 717, October 2022.

McFarlan F. W., & Nolan R. L. (1995). How to manage an IT outsourcing alliance. *MIT Sloan Management Review*, *36*(2), 9.

Pellitteri R., Parrini R., Cafarotti C. & De Vendictis B. A. (2023), "L'Open Banking nel sistema dei pagamenti: evoluzione infrastrutturale, innovazione e sicurezza, prassi di vigilanza e sorveglianza", *Banca d'Italia - Mercati, infrastrutture, sistemi di pagamento*, No. 31, March 2023.

Papers published in the 'Markets, Infrastructures, Payment Systems' series

n. 1 TIPS - TARGET Instant Payment Settlement – The Pan-European Infrastructure for the Settlement of Instant Paymentsi, *by Massimiliano Renzetti, Serena Bernardini, Giuseppe Marino, Luca Mibelli, Laura Ricciardi and Giovanni M. Sabelli* (Institutional Issues)

n. 2 Real-Time Gross Settlement systems: breaking the wall of scalability and high availability, *by Mauro Arcese, Domenico Di Giulio and Vitangelo Lasorella* (Research Papers)

n. 3 Green Bonds: the Sovereign Issuers' Perspective, *by Raffaele Doronzo, Vittorio Siracusa and Stefano Antonelli* (Research Papers)

n. 4 T2S - TARGET2-Securities – The pan-European platform for the settlement of securities in central bank money, *by Cristina Mastropasqua, Alessandro Intonti, Michael Jennings, Clara Mandolini, Massimo Maniero, Stefano Vespucci and Diego Toma* (Institutional Issues)

n. 5 The carbon footprint of the Target Instant Payment Settlement (TIPS) system: a comparative analysis with Bitcoin and other infrastructures, *by Pietro Tiberi* (Research Papers)

n. 6 Proposal for a common categorisation of IT incidents, *by Autorité de Contrôle Prudentiel et de Résolution, Banca d'Italia, Commissione Nazionale per le Società e la Borsa, Deutsche Bundesbank, European Central Bank, Federal Reserve Board, Financial Conduct Authority, Ministero dell'Economia e delle Finanze, Prudential Regulation Authority, U.S. Treasury* (Institutional Issues)

n. 7 Inside the black box: tools for understanding cash circulation, *by Luca Baldo, Elisa Bonifacio, Marco Brandi, Michelina Lo Russo, Gianluca Maddaloni, Andrea Nobili, Giorgia Rocco, Gabriele Sene and Massimo Valentini* (Research Papers)

n. 8 The impact of the pandemic on the use of payment instruments in Italy, *by Guerino Ardizzi, Alessandro Gambini, Andrea Nobili, Emanuele Pimpini and Giorgia Rocco* (Research Papers) (in Italian)

n. 9 TARGET2 – The European system for large-value payments settlement, *by Paolo Bramini, Matteo Coletti, Francesco Di Stasio, Pierfrancesco Molina, Vittorio Schina and Massimo Valentini* (Institutional Issues) (in Italian)

n. 10 A digital euro: a contribution to the discussion on technical design choices, *by Emanuele Urbinati, Alessia Belsito, Daniele Cani, Angela Caporrini, Marco Capotosto, Simone Folino, Giuseppe Galano, Giancarlo Goretti, Gabriele Marcelli, Pietro Tiberi and Alessia Vita* (Institutional Issues)

n. 11 From SMP to PEPP: a further look at the risk endogeneity of the Central Bank, *by Marco Fruzzetti, Giulio Gariano, Gerardo Palazzo and Antonio Scalia* (Research Papers)

n. 12 TLTROs and collateral availability in Italy, *by Annino Agnes, Paola Antilici and Gianluca Mosconi* (Research Papers) (in Italian)

n. 13 Overview of central banks' in-house credit assessment systems in the euro area, *by* L*aura Auria, Markus Bingmer, Carlos Mateo Caicedo Graciano, Clémence Charavel, Sergio Gavilá, Alessandra Iannamorelli, Aviram Levy, Alfredo Maldonado, Florian Resch, Anna Maria Rossi and Stephan Sauer* (Institutional Issues)

n. 14 The strategic allocation and sustainability of central banks' investment, *by Davide Di Zio, Marco Fanari, Simone Letta, Tommaso Perez and Giovanni Secondin* (Research Papers) (in Italian)

n. 15 Climate and environmental risks: measuring the exposure of investments, *by Ivan Faiella, Enrico Bernardini, Johnny Di Giampaolo, Marco Fruzzetti, Simone Letta, Raffaele Loffredo and Davide Nasti* (Research Papers)

n. 16 Cross-Currency Settlement of Instant Payments in a Multi-Currency Clearing and Settlement Mechanism, *by Massimiliano Renzetti, Fabrizio Dinacci and Ann Börestam* (Research Papers)

n. 17 What's ahead for euro money market benchmarks?, *by Daniela Della Gatta* (Institutional Issues) (in Italian)

n. 18 Cyber resilience per la continuità di servizio del sistema finanziario, *by Boris Giannetto and Antonino Fazio* (Institutional Issues) (in Italian)

n. 19 Cross-Currency Settlement of Instant Payments in a Cross-Platform Context: a Proof of Concept, *by Massimiliano Renzetti, Andrea Dimartina, Riccardo Mancini, Giovanni Sabelli, Francesco Di Stasio, Carlo Palmers, Faisal Alhijawi, Erol Kaya, Christophe Piccarelle, Stuart Butler, Jwallant Vasani, Giancarlo Esposito, Alberto Tiberino and Manfredi Caracausi* (Research Papers)

n. 20 Flash crashes on sovereign bond markets – EU evidence, *by Antoine Bouveret, Martin Haferkorn, Gaetano Marseglia and Onofrio Panzarino* (Research Papers)

n. 21 Report on the payment attitudes of consumers in Italy: results from ECB surveys, *by Gabriele Coletti, Alberto Di Iorio, Emanuele Pimpini and Giorgia Rocco* (Institutional Issues)

n. 22 When financial innovation and sustainable finance meet: Sustainability-Linked Bonds, *by Paola Antilici, Gianluca Mosconi and Luigi Russo* (Institutional Issues) (in Italian)

n. 23 Business models and pricing strategies in the market for ATM withdrawals, *by Guerino Ardizzi and Massimiliano Cologgi* (Research Papers)

n. 24 Press news and social media in credit risk assessment: the experience of Banca d'Italia's In-house Credit Assessment System, *by Giulio Gariano and Gianluca Viggiano* (Research Papers)

n. 25 The bonfire of banknotes, *by Michele Manna* (Research Papers)

n. 26 Integrating DLTs with market infrastructures: analysis and proof-of-concept for secure DvP between TIPS and DLT platforms, *by Rosario La Rocca, Riccardo Mancini, Marco Benedetti, Matteo Caruso, Stefano Cossu, Giuseppe Galano, Simone Mancini, Gabriele Marcelli, Piero Martella, Matteo Nardelli and Ciro Oliviero* (Research Papers)

n. 27 Statistical and forecasting use of electronic payment transactions: collaboration between Bank of Italy and Istat, *by* Guerino Ardizzi and Alessandra Righi (Institutional Issues) (in Italian)

n. 28 TIPS: a zero-downtime platform powered *by* automation, by *Gianluca Caricato, Marco Capotosto, Silvio Orsini and Pietro Tiberi* (Research Papers)

n. 29 TARGET2 analytical tools for regulatory compliance, *by Marc Glowka, Alexander Müller, Livia Polo Friz, Sara Testi, Massimo Valentini and Stefano Vespucci* (Institutional Issues)

n. 30 The security of retail payment instruments: evidence from supervisory data, *by Massimiliano Cologgi* (Research Papers)

n. 31 Open Banking in the payment system: infrastructural evolution, innovation and security, supervisory and oversight practices, *by Roberto Pellitteri, Ravenio Parrini, Carlo Cafarotti and Benedetto Andrea De Vendictis* (Institutional Issues) (in Italian)

n. 32 Banks' liquidity transformation rate: determinants and impact on lending, *by Raffaele Lenzi, Stefano Nobili, Filippo Perazzoli and Rosario Romeo* (Research Papers)

n. 33 Investor behavior under market stress: evidence from the Italian sovereign bond market, *by Onofrio Panzarino* (Research Papers)

n. 34 Siamese neural networks for detecting banknote printing defects, *by Katia Boria, Andrea Luciani, Sabina Marchetti and Marco Viticoli* (Research Papers) (in Italian)

n. 35 Quantum safe payment systems, *by Elena Bucciol and Pietro Tiberi*

n. 36 Investigating the determinants of corporate bond credit spreads in the euro area, *by Simone Letta and Pasquale Mirante*

n. 37 Smart Derivative Contracts in DatalogMTL, *by Andrea Colombo, Luigi Bellomarini, Stefano Ceri and Eleonora Laurenza*

n. 38 Making it through the (crypto) winter: facts, figures and policy issues, *by Guerino Ardizzi, Marco Bevilacqua, Emanuela Cerrato and Alberto Di Iorio*

n. 39 The Emissions Trading System of the European Union (EU ETS), *by Mauro Bufano, Fabio Capasso, Johnny Di Giampaolo and Nicola Pellegrini* (in Italian)

n. 40 Banknote migration and the estimation of circulation in euro area countries: the italian case, *by Claudio Doria, Gianluca Maddaloni, Giuseppina Marocchi, Ferdinando Sasso, Luca Serrai and Simonetta Zappa* (in Italian)

n. 41 Assessing credit risk sensitivity to climate and energy shocks, *by Stefano Di Virgilio, Ivan Faiella, Alessandro Mistretta and Simone Narizzano*

n. 42 Report on the payment attitudes of consumers in italy: results from the ecb space 2022 survey, *by Gabriele Coletti, Alberto Di Iorio, Emanuele Pimpini and Giorgia Rocco*

n. 43 A service architecture for an enhanced Cyber Threat Intelligence capability and its value for the cyber resilience of Financial Market Infrastructures, *by Giuseppe Amato, Simone Ciccarone, Pasquale Digregorio and Giuseppe Natalucci*

n. 44 Fine-tuning large language models for financial markets via ontological reasoning, *by Teodoro Baldazzi, Luigi Bellomarini, Stefano Ceri, Andrea Colombo, Andrea Gentili and Emanuel Sallinger*

n. 45 Sustainability at shareholder meetings in France, Germany and Italy, *by Tiziana De Stefano, Giuseppe Buscemi and Marco Fanari* (in Italian)

n. 46 Money market rate stabilization systems over the last 20 years: the role of the minimum reserve requirement, *by Patrizia Ceccacci, Barbara Mazzetta, Stefano Nobili, Filippo Perazzoli and Mattia Persico*