TOOLKIT

Access to payment systems for non-bank payment service providers

1. Considerations for jurisdictions enabling NBPSP access
2. NBPSP checklist to obtain direct access to payment systems



Cross-border Payments Interoperability and Extension (PIE) task force

This report was prepared by a selection of PIE task force members*, with additional inputs and comments from other parties. The views expressed in this report do not necessarily reflect those of the Bank for International Settlements (BIS), the BIS Committee on Payments and Market Infrastructures (CPMI), its member central banks, or the whole PIE Task Force and its members.

*Led by Magali Van Bulck

Executive summary

Access to payment systems for non-bank payment service providers (NBPSPs) is an increasingly important policy consideration as jurisdictions seek to improve competition, resilience, efficiency and financial inclusion in payments. In the 2025 CPMI-FSB monitoring survey covering 82 jurisdictions, 45% of fast payment systems (FPS) and 39% of real-time gross settlement (RTGS) systems already provided direct access to authorised non-bank PSPs. In the months following the survey, that share was expected to reach nearly 60%.

Historically, direct access to core payment infrastructures has often been limited to banks, requiring NBPSPs to rely on direct participants ("sponsor banks") to connect indirectly. Such arrangements can be efficient and appropriate for some providers, but may also introduce dependencies, costs, and concentration risks. Direct participation can reduce these dependencies and give NBPSPs greater control over payment processing and settlement. However, it can also entail greater liquidity, operational and risk-management responsibilities for NBPSPs. If access to central bank settlement accounts is involved, it also has implications for the central bank's operational, supervisory and balance-sheet responsibilities.

This toolkit does not take a position on whether jurisdictions should expand direct access to payment systems or to central bank settlement accounts. That is a prior policy choice requiring a jurisdiction specific assessment of the benefits, risks and institutional implications since different access and settlement arrangements involve different trade-offs. The toolkit focuses on practical considerations for jurisdictions that have concluded that enabling NBPSP access is appropriate. Building on the G20 Roadmap for Enhancing Cross-Border Payments and prior work by the CPMI and the PIE task force, this toolkit provides a practical framework for authorities and payment system operators (PSOs) considering the design and implementation of direct access models for NBPSPs. It also provides guidance for NBPSPs assessing whether direct participation is appropriate or feasible for them, drawing on real-world experiences from NBPSPs who have already done so. The toolkit is structured in two parts.

Part 1: Enabling direct access - considerations for authorities
Drawing on global experience from jurisdictions that have already implemented direct NBPSP participation, Part 1 presents a range of policy and design options for jurisdictions who have decided to enable direct NBPSP participation.

Considerations motivating changes to NBPSP access arrangements are consistent among surveyed jurisdictions and include:

- Promoting competition and innovation, including by enabling new entrants and reducing their reliance on sponsor banks.
- Addressing concentration and resilience risks, where a significant number of NBPSPs depend on a small number of direct participants.
- Improving efficiency and lowering costs if intermediaries can be removed, shortening transaction chains.
- Supporting financial inclusion and digitalisation, particularly in markets where NBPSPs play an important role in providing payment services.

These desired benefits need to be considered alongside the potential risks and costs associated with different participation models, including implications for liquidity management, operational resilience, financial crime controls, safeguarding arrangements, supervision and, where relevant, access to central bank money.

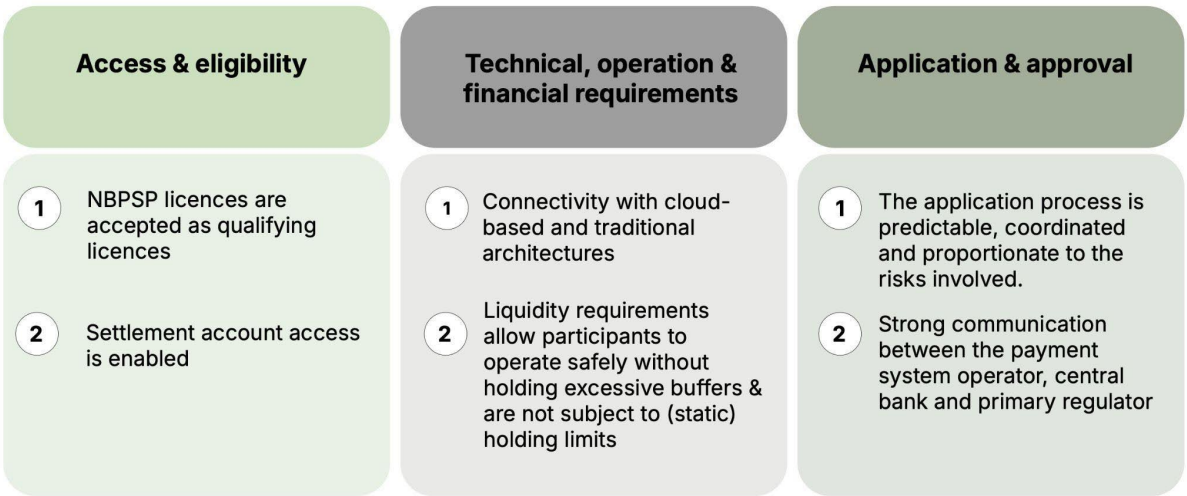
Jurisdictions that want to enable direct access for NBPSPs, typically consider the following design choices:

- Legal and regulatory foundations: Create legal and regulatory clarity for PSOs and NBPSPs, including appropriate licensing, oversight and supervision, AML/CFT compliance, safeguarding and governance requirements.
- Access and settlement models: Determine the type of access PSOs can provide to NBPSPs, such as technical access only, settlement through another participant or full direct access with central bank settlement accounts.
- Risk-based safeguards: Establish requirements based on the risks posed by participants and their activities, while maintaining appropriate standards for operational resilience, liquidity management and financial crime controls as for incumbent participants.
- Operational and technical requirements: Maintain robust security and resilience standards while considering technology-neutral approaches that support modern, cloud-based and API-driven architectures to be accommodating to more business models (including those of newer entrants).
- Supervisory and institutional coordination: Strengthen cooperation between authorities and PSOs to ensure consistent oversight and avoid duplication.
- Transparent application processes: Encourage clear eligibility criteria, onboarding guidance and predictable timelines to reduce uncertainty for applicants.

Jurisdictions that have expanded access have generally sought to adapt participation requirements to different business models without lowering standards. Instead, they adapted existing safeguards to non-bank business models, ensuring that system integrity is maintained while enabling broader participation.

The common themes can be summarised as follows:

Enabling conditions for NBPSP access to payment systems



Part 2: NBPSP checklist - obtaining and operating direct access

Part 2 provides a practical guide for NBPSPs considering direct participation, covering the full lifecycle from initial business case to post-launch operations. A central element of this evaluation is the comparison between direct and indirect participation. The checklist outlines key requirements across governance, liquidity, technical integration and compliance, while also highlighting common challenges observed in practice. These include navigating requirements originally designed for banks, interpreting incomplete or unclear payment system documentation, managing prefunding and liquidity constraints with conservative buffers, and building and operating resilient, always-on infrastructure. NBPSPs may also face operational challenges during onboarding,

including limited transparency on timelines, fragmented coordination between authorities, and constrained testing environments.

Overall, the experience across jurisdictions shows that NBPSPs can participate directly in payment systems and unlock benefits, while system integrity can be maintained if the relevant risks are appropriately identified and managed. However, doing so requires addressing practical challenges through proportionate, risk-based safeguards, clear and more transparent processes, and modern, flexible infrastructure and connectivity models that can be adapted to cloud-based setups. This report offers practical suggestions for authorities, PSOs and NBPSPs.

NBPSP checklist	
Decision-making criteria & discovery	**Strategic & business rationale** ● Develop a clear business case for direct access ● Compare direct vs indirect/sponsor model **Payment system discovery** ● Identify whether a settlement account is required, optional or not permitted ● Identify payment system rules and operational requirements ● Identify third party vendors to facilitate the connectivity and integration
Pre-application checklist	**Legal & regulatory preparation** ● Confirm that the correct regulatory licence and permissions are in place **Governance & risk framework** ● Document risk management and operational resilience frameworks specifically for payment system participation ● Create an incident response policy for payment system participation ● Establish an outsourcing framework for payment system-related dependencies (cloud or third-party dependencies) **Financial requirements** ● Prepare a capital impact assessment ● Create a liquidity plan for prefunding/settlement **Technical architecture readiness** ● Define the integration pattern (direct messaging, gateway provider) ● Ensure payment messaging and payment flow readiness **Discovery questionnaires** ● Complete the PSO due diligence questionnaire ● Complete the central bank risk questionnaire (if required) ● Complete the self-assessment against payment system rulebooks
Application and approval checklist	**PSO approval** ● Submit membership application ● Sign the participation agreement and confirm rulebook compliance ● Agree payment system & associated fees *Risk & controls* ● Fraud controls reviewed and approved ● Operational risk controls validated

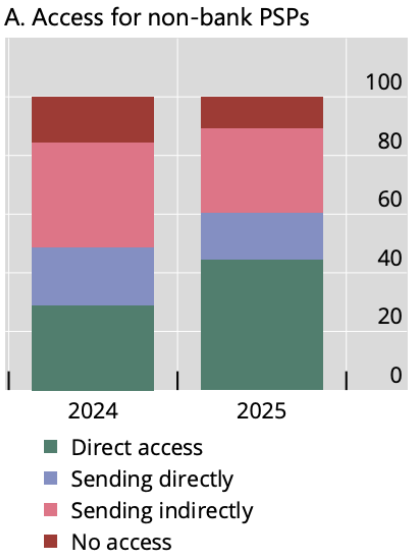
	● Cyber security review passed *Financial arrangements* ● Confirm the settlement model ● Finalise collateral or prefunding arrangements (if applicable) **Regulatory approval** ● Submit a formal regulatory notification or permission request ● Pass a regulatory assessment to obtain a non-objection **Central bank approval (where central bank account or settlement access required)** ● Settlement account application approved (if applicable) ● Confirm reporting obligations and obtain testing certification
Technical setup and testing checklist	**Connectivity setup** ● Determine network routing ● Define IP configuration ● Establish transport protocols and message exchange ● Set up security architecture and key management ● Optimise latency and performance **Functional setup** ● Implement message mapping and validation ● Design and automate unhappy path handling ● Implement liquidity and settlement logic ● Establish automated reconciliation ● Ensure adequate load handling and capacity management **Testing and certification** ● Complete functional certification testing ● Test failure scenarios and disaster recovery
Go-live	● Roll out gradually and in a controlled way (via penny testing)
Post-launch	**Maintenance** ● Manage payment system and mandatory updates ● Maintain certificate and key lifecycle processes ● Conduct recurring disaster recovery and resilience testing ● Maintain liquidity and financial controls ● Meet ongoing compliance and reporting obligations ● Manage operational and governance participation

Introduction

The G20 Roadmap for Enhancing Cross-Border Payments, launched in October 2020, aims to achieve 4 main outcomes: lower cost, higher speed, improved access and increased transparency in cross-border payments. The Roadmap initially included 19 Building Blocks to achieve those outcomes, including Building Block 10: improving (direct) access to payment systems. Building on this initial work, the Roadmap has focused on priority actions since 2023.

As the Bank of England highlights, *"increased direct access to payment systems can speed up payments and reduce costs through reducing the number of intermediaries a payment goes through"*[1], which explains its crucial contribution towards improving cross-border payments. Similarly, the Committee on Payments and Market Infrastructures (CPMI) sets out additional benefits, including that "*expanded access can [...] lead to greater choice and better pricing for end users and improve financial inclusion. PSPs with direct access can benefit from reduced funding costs since they may not have to prefund at the same levels as with some indirect arrangements. The financial system more broadly could benefit from enhanced settlement risk mitigation and potential financial stability benefits through the reduction of tiered arrangements and a more diverse and resilient ecosystem*."[2]

Since the introduction of the G20 Roadmap, there has been meaningful progress in providing direct access to payment systems for Non-Bank Payment Service Providers (NBPSPs) across G20 markets and beyond. According to the BIS Bulletin 119, *"cross-country monitoring data indicate that FPS increasingly offer direct access to non-bank PSPs, fostering competition."*[3] Results of the CPMI-FSB 2025 monitoring survey further substantiate the expansion of direct access, with a notable increase of FPS that have enabled direct access in 2025 compared to 2024, as shown in the graph (right). *(Direct access = direct access with or without access to issuing credit; sending directly = can send directly without settlement account; sending indirectly = can send indirectly without settlement account).*[4]



Under the CPMI's Cross-border payments interoperability and extension (PIE) task force, previous work resulted in the report titled *"Expanding Access to Payment Systems: Considerations for a Path Forward"*[5]. This report laid the groundwork for identifying key considerations for improving direct access to payment systems for banks and NBPSPs. It highlighted the potential benefits of expanded access, including increased competition, reduced transaction costs, and improved financial inclusion, while also addressing the challenges and risks involved. The report includes considerations for regulators, central banks and PSOs considering the expansion of access to their payment system.

Building on this foundational work, this toolkit aims to offer a practical guide for enabling direct access for a wider number of participants, with a focus on NBPSPs.

[1] https://www.bankofengland.co.uk/report/2025/rtgs-and-chaps-annual-report-2024-25
[2] https://www.bis.org/cpmi/publ/d202.pdf
[3] https://www.bis.org/publ/bisbull119.pdf
[4] https://www.bis.org/cpmi/publ/brief13.pdf
[5] https://www.bis.org/pages/cpmi-cross-border-payments-programme/pietf-payment-systems-feb-2026.pdf

The first part of the toolkit presents options for enabling non-bank access to payment systems. These considerations cover a range of access models and design choices, allowing jurisdictions to tailor their strategies to local market needs and risk considerations. By exploring different access models and design options, this toolkit provides a guide for stakeholders aiming to drive positive change in the payment ecosystem. Through interviews with central banks[6] who have implemented direct access for NBPSPs or are taking steps in this direction, this report illustrates how jurisdictions from across the world approached this topic, providing valuable insights and lessons learned.

In the second part of the toolkit, we set out a checklist for NBPSPs who wish to explore direct access to a payment system. From building out the business case to post-launch maintenance, every step of the process is set out in detail and is supplemented by practical NBPSP experience. Many steps include challenges NBPSPs have faced. These challenges may not be unique to NBPSPs but can apply to (prospective) participants across the board. In addition, each step includes considerations for PSOs and authorities to streamline the process for (aspiring) NBPSP participants. These considerations can apply to those who already enable NBPSPs to join their payment systems, as well as those building out the frameworks from scratch.

The goal is to enable stakeholders to make informed decisions that maintain system integrity while promoting openness, competition and resilience, ultimately benefiting consumers and businesses alike.

[6] Seven respondents, representing payment systems from every continent.

PART 1: ENABLING DIRECT ACCESS FOR NON-BANK PAYMENT SERVICE PROVIDERS (NBPSPs): CONSIDERATIONS FOR AUTHORITIES & PAYMENT SYSTEM OPERATORS

In 2022, the CPMI developed a self-assessment framework for jurisdictions and PSOs who are considering expanding access to key payment systems.[7] This work enables jurisdictions to assess *whether* they should expand access to payment systems for a wider range of participants, including NBPSPs. The self-assessment also includes considerations and examples from other jurisdictions around settlement finality, participant eligibility criteria and other factors, which can serve as inspiration for jurisdictions undertaking their own self-assessments. This document explores further *how* they can achieve this, building on the experiences and policies of other jurisdictions that already enable direct access for NBPSPs.

This section is informed by questionnaire responses from central banks who have direct access frameworks for NBPSPs in place or are in the process of enabling this, as well as publicly available resources from jurisdictions that have enabled NBPSP access.

1. Why jurisdictions expand access to NBPSPs: policy drivers

The decision to enable direct access is typically driven by four consistent objectives:

Driver	Description
Promoting competition & innovation	Traditionally, NBPSPs have had to rely on banks - often direct competitors - to sponsor their access to a payment system, which some central banks recognise can create structural barriers to competition. By enabling a wider range of participants to access payment infrastructure directly, NBPSP entrants can challenge incumbents and drive improvements in price, quality and functionality. NBPSPs may also adopt new services, overlays or other forms of innovation more quickly and put pressure on other participants to follow suit.
Reducing concentration risk & improving resilience	Another key driver for expanding direct access to NBPSPs is to strengthen the resilience of the payment system by reducing concentration and dependence on a small number of sponsor banks. In many jurisdictions, indirect access models result in a limited number of large banks providing an indirect connection for a wide range of NBPSPs, which introduces concentration risk. If one bank fails or is in duress, all the NBPSPs that depend on it face the same issue. Reducing single points of failure lowers the risk to the overall resilience of the payment system.
Improving efficiency & reducing (intermediary) costs	While indirect access models enable NBPSPs to participate in payment systems, they introduce additional layers into the payment chain. These arrangements can create inefficiencies and dependencies. Payments routed through sponsor banks may involve extra steps in validation and reconciliation, increasing processing time. At the same time, NBPSPs have to enter into a commercial agreement with their sponsor bank, which usually sets a per transaction cost. These fees can add up, reducing the competitiveness of the NBPSP and increasing costs for end-users.
Supporting financial inclusion & digitalisation	In many jurisdictions, particularly emerging and fast-growing digital economies, expanding access to payment systems for NBPSPs is closely linked to broader objectives around financial inclusion and digitalisation. Policymakers increasingly recognise that NBPSPs play a central role in extending financial services to underserved people and businesses. As a result, restricting access to core payment infrastructure to banks alone can limit the reach and effectiveness of national payment systems.

[7] https://www.bis.org/cpmi/publ/d202.pdf

Jurisdictions that have enabled direct access weighed these policy drivers against potential risks to their payment systems. More information about the barriers and risks associated with expanding direct access can be found in the CPMI's *Improving access to payment systems for cross-border payments: best practices for self-assessments*.[8]

2. How jurisdictions can open access to NBPSPs: enabling considerations

2.1. Access/eligibility criteria

2.1.1. Licence criteria

Risk-proportionate frameworks can recognise NBPSP licences for full direct participation, moving beyond static lists of eligible licence categories and focusing on firms' capabilities.

In most jurisdictions, participation in payment systems is limited to certain (bank) licence types. For jurisdictions that want to enable direct access for NBPSPs, the starting point is therefore to expand the eligible licence types, which were often centred around banks or other deposit-taking institutions, to also include other types of firms that already provide regulated payment services in the market. This may include but is not limited to payment institutions, electronic money institutions/issuers, (international) money transfer operators, and could require changes to the legal or regulatory framework.

Recognising these NBPSP licence types for direct participation - provided the NBPSP also meets the payment system's operational, liquidity and risk management requirements - removes the need for a NBPSP to exclusively rely on a sponsor bank to facilitate payments. Sponsor banks typically provide "indirect" access to payment systems, clearing and settling payments on behalf of a NBPSP's customers. While it is important that indirect access remains an option, enabling NBPSPs to connect directly reduces the interdependence and concentration risk of too many NBPSPs connecting via a few sponsor banks. Some payment systems also allow directly connected NBPSPs to enable indirect access for other PSPs. This can reduce concentration risk and promote competition.

Jurisdictions that impose no additional requirements for direct access beyond a NBPSP license typically have the central bank responsible for supervising NBPSPs. Especially where the central bank is not the NBPSP supervisory authority, additional assessments may be required. In one jurisdiction, additional safeguards require NBPSPs to have operated for at least nine months before their application is fully assessed. This requirement is intended to ensure that they have attained a sufficient level of maturity and familiarity with the market before accessing the payment system directly.

A different jurisdiction previously allowed access to non-regulated entities, but this was rolled back due to heightened risk to the resilience of the payment system. Access is now limited to entities regulated by the central bank. This experience highlights the importance of establishing minimum participation criteria that provide the necessary safeguards. Licensed entities require high levels of compliance to ensure they meet all their regulatory obligations, including stringent security and operational resilience requirements. These requirements, in addition to a regulatory assessment prior to being granted access, mitigate risks to the payment system.

A further jurisdiction which did not offer direct NBPSP participation due to NBPSPs not being subject to prudential supervision, has proposed a new form of licence for NBPSPs seeking direct access to payment systems. This licence type would entail a set of proportionate regulatory and supervisory arrangements, to generate confidence that NBPSPs directly involved in the clearing and settlement of payments are managing the

[8] https://www.bis.org/cpmi/publ/d202.pdf

associated risks appropriately. These reforms will be followed by the introduction of common access requirements, which will set industry-wide standards for access to payment systems, covering critical operational areas, including data security, governance, risk management, capital adequacy, liquidity management, and business continuity planning.

The focus on risk-mitigating safeguards is echoed by another jurisdiction. They noted that the primary bottlenecks and reasons for rejection in the application process largely related to the lack of clarity regarding pre-funding, liquidity management, settlement process, and safeguarding. In particular, this jurisdiction scrutinises an NBPSP's reliance on sponsor banks for liquidity controls, and cautioned that an over-reliance on these intermediaries can undermine the independence and concentration risk reduction that direct access intended to achieve.

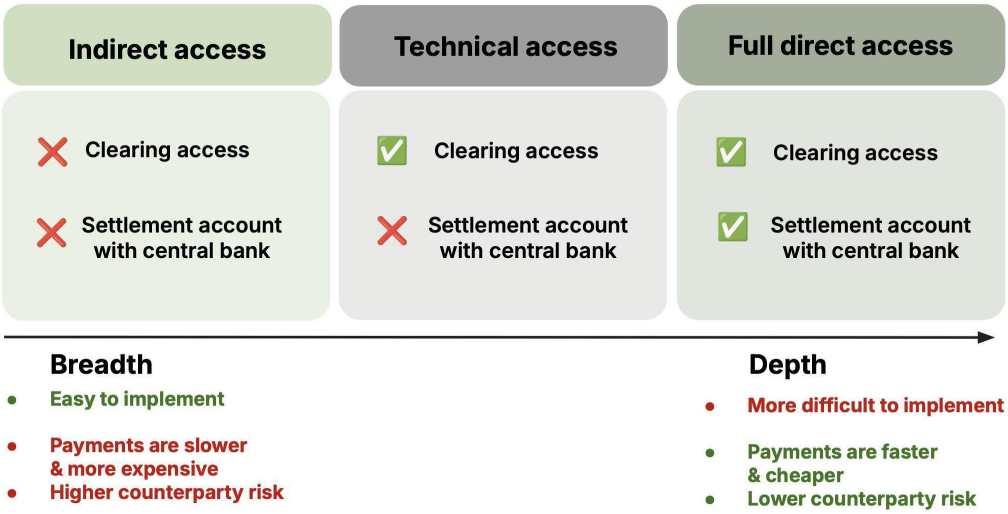
Jurisdictions that have expanded access have often moved beyond static lists of eligible licence types and instead adopted activity-based, risk proportionate frameworks. These frameworks assess whether a firm can safely perform functions required of a direct payment system participant, rather than whether it holds a specific type of licence. Under this more advanced approach, the payment system framework does not merely say which legal entities can participate. It also sets out which regulated payment activities and supervisory outcomes qualify a firm for direct access. This is especially useful in jurisdictions where the licensing perimeter is fragmented or where several different licence types may cover similar payment activities.

A formal mechanism between the regulator and the central bank or PSO can support this, allowing the PSO and relevant regulators to minimise duplication in their assessment. As a result, the application process should be more predictable and avoid duplicated due diligence.

2.1.2. Settlement account access

> 💡 **Direct access to central bank settlement accounts enables eligible NBPSPs to participate fully without intermediaries or sponsor bank concentration risks.**

In addition to direct access to payment systems, direct access to central bank settlement accounts enables NBPSPs to both send payment instructions (payment system access) and settle the resulting obligations in central bank money via an account held with the central bank (central bank account access). Being able to settle in central bank money can reduce the risks associated with reliance on commercial bank sponsors and allows non-banks to manage their own liquidity. It also comes with increased liquidity management, operational resilience and settlement responsibility for the NBPSP, and brings the central bank into a direct relationship with a wider set of entities. The implications for central banks may vary depending on the type of payment system and the settlement arrangements in place. In particular, access to wholesale payment systems may raise broader liquidity, balance-sheet and policy considerations, which require a separate assessment by the relevant central bank.



Jurisdictions seeking to ensure that NBPSPs can participate fully in the payment system without reliance on intermediaries may consider allowing eligible NBPSPs to open a dedicated settlement account with the central bank. As part of the application process, the central bank would typically assess if the NBPSP meets the relevant operational, liquidity and risk management requirements.

This full direct access model mitigates the concentration risk where a major sponsor bank's outage freezes the operations of all the NBPSPs it supports. This is increasingly important as NBPSPs grow to become more relevant nodes in the economy. This is consistent with CPMI analysis, which highlights that direct access to central bank money can reduce transaction chains and mitigate credit and liquidity risks associated with tiered participation.[9] These settlement accounts may be restricted to settlement purposes only or may include additional services, such as intraday liquidity, depending on central bank policy.

In practice, several jurisdictions have already implemented this approach, among them those with high levels of NBPSP participation. In Mexico's SPEI, 50% of direct participants are now NBPSPs,[10] while in the UK's Faster Payment System roughly one third of participants are NBPSPs.[11] The Bank of England revised its policy in 2017 to allow NBPSPs to open settlement accounts, reducing reliance for settlement on commercial sponsors . In Brazil's Reserves Transfer System (STR) NBPSPs have been able to connect directly since 2009 and the Central Bank of Brazil (BCB) continued that same approach in SPI (Instant Payment System), which settles Pix transactions. In the Philippines, the Bangko Sentral ng Pilipinas (BSP) allows non-bank electronic money issuers (EMIs) to be direct participants in PhilPaSS Plus, enabling them to settle InstaPay and PESONet obligations directly in central bank money. In Türkiye, NBPSPs have been able to directly access FAST, the FPS, since November 2023. They can both send payment instructions (technical access) and open a settlement account at the Central Bank of the Republic of Türkiye to settle the resulting obligations (settlement access) in central bank money. In Japan, non-bank fund transfer service providers can access the Zengin system directly since 2025 and open settlement accounts at the Bank of Japan, subject to a decision on a case-by-case basis by the Bank of Japan Policy Board. Similar models are now being operationalised in Canada and in the European Union, where recent regulatory changes enable NBPSPs to access payment systems and settlement accounts if they meet all the criteria.

[9] https://www.bis.org/cpmi/publ/d202.pdf

[10] https://anterior.banxico.org.mx/servicios/participantes-spei-banco-me.html

[11] https://www.wearepay.uk/what-we-do/payment-systems/faster-payment-system/payment-system-participant-list/

Certain jurisdictions have complemented this model with threshold-based requirements for direct participation. For example, in Brazil's Pix and Mexico's SPEI, participation becomes mandatory once a PSP exceeds 500,000 active customer accounts. In the UK's RTGS, a financial institution is expected to directly connect once they account for 2% of payment value (i.e. where a PSP's average daily CHAPS payment value sent and received exceeds 2% of the average daily value of CHAPS payments). These approaches help reduce concentration risk and ensure that the largest and most critical PSPs operate with full independence and accountability within the system.

Some jurisdictions enable a technical access only model (no settlement account with the central bank). Under this model, NBPSPs can connect directly to the payment system to exchange messages, but settlement continues to take place via a sponsor bank. An example for the technical access approach is Singapore, where NBPSPs can connect directly to FAST and PayNow but must rely on a settlement institution for final settlement in central bank money. This lowers the initial barrier to entry and allows firms to begin integrating with the payment system before building full treasury and liquidity capabilities. It can also be introduced and implemented more quickly than full settlement access. Technical only access, however, might not deliver the same benefits as settlement access, as NBPSPs remain dependent on commercial banks.

A different approach is taken in Canada, where both technical and fully direct access are available. This hybrid approach enables a participant to choose which access suits them best, while ensuring that NBPSPs are provided with the ability to settle directly.

2.2. Technical, operational & financial considerations

> 💡 **Consistent, risk-based requirements focus on NBPSPs' governance, liquidity and operational capabilities, while allowing flexible, technology-neutral compliance.**

Across jurisdictions surveyed, central banks consistently identify technical, operational and financial requirements as the main practical barriers to participation. In many cases, these requirements were originally designed for banks and reflect legacy assumptions around infrastructure, network configurations, operating models and balance sheet setup. These can include requirements for dedicated leased lines, on-premise data centres, proprietary messaging protocols and physical hardware security modules (HSMs), as well as conservative prefunding or collateral arrangements.

Some central banks reported that these requirements do not necessarily pose greater challenges for NBPSPs than for banks. Instead, differences in operational maturity, readiness and experience with payment system integration tend to be the main factors influencing successful onboarding. Similarly, one jurisdiction noted that the ability of participants to demonstrate internal governance, liquidity management and operational capability are important criteria to assess readiness to participate directly.

As a result, jurisdictions that have expanded access have generally focused on:

- ensuring that requirements are risk-based and consistently applied, applying the same requirements to all participants, regardless of whether an entity is a bank or a NBPSP.
- assessing firms based on their ability to manage risk, rather than their licence type.
- allowing flexibility in how requirements are met, taking a more technologically neutral approach.

2.2.1. Connectivity models and infrastructure

Flexible, outcome-focused and technology-neutral connectivity models, based on third-party and direct options, can enable NBPSPs' participation while reducing barriers to entry.

Central banks report a range of connectivity approaches across payment systems, including direct connections to central infrastructure, connections via certified network providers and the use of intermediary gateways. Jurisdictions that have enabled direct access typically provide at least one clearly defined connectivity model that allows participants to connect directly to the payment system infrastructure, supported by comprehensive technical documentation. This is the baseline required to enable full direct participation.

In practice, establishing direct connectivity can be complex. One central bank highlighted that connecting directly to its payment system requires multiple network connections and redundancy arrangements, with only a limited number of network providers available and approved (monopolies or duopolies of this service are fairly common in other jurisdictions, too). This has led to the emergence of specialised technology service providers offering connectivity as a managed service, increasing competition and reducing barriers for smaller participants. However, in some cases this set-up is not compatible with a PSP's cloud-based infrastructure, which tends to be more common among newer participants, and can therefore act as a barrier to entry. Another central bank similarly noted that participants are able to choose between direct connectivity and the use of third-party providers, reflecting a flexible approach to integration design. For example, a large NBPSP with an experienced engineering team may prefer building its own direct connection, while a smaller firm entering a new market may use a gateway provider to reduce implementation time. This flexibility is important.

In addition, jurisdictions where NBPSP direct connectivity is enabled, have moved away from prescribing specific infrastructure (or are in the process of doing so). A more effective approach is to define what needs to be achieved. A focus on outcomes such as secure encryption of messages, certified key storage, or defined uptime, allows participants to use different technologies to meet the same objective. For example, one jurisdiction is currently working to introduce optional cloud connectivity for direct participants as an alternative option to hosting a custom-built payment gateway. This enhances compatibility with (prospective) participants' cloud-based infrastructure and reduces the barrier for entry for cloud-based participants.

More detailed connectivity considerations can be found in Part 2, section 4.1 Connectivity setup.

2.2.2. Holding limits and liquidity design

Dynamic and risk appropriate liquidity arrangements enable NBPSPs to meet settlement obligations during growth and transaction peaks without holding excessive buffers.

Financial requirements, particularly those related to liquidity and prefunding, are identified by central banks as a key consideration for direct access. Several jurisdictions require participants to demonstrate their ability to manage settlement capacity, including forecasting transaction volumes and ensuring sufficient balances are available to meet obligations.

In some cases, settlement account access is paired with maximum holding limits or prefunding caps. Where these limits are static or infrequently updated, they can constrain the ability of fast-growing participants to process payments, particularly during periods of rapid growth or peak transaction activity.

Jurisdictions that have enabled access typically ensure that participants can maintain sufficient balances to meet their settlement obligations, including overnight where required to support continuous operation. This is

particularly important for payment systems that operate on a 24/7 basis. In more advanced frameworks, liquidity limits are reviewed on a rolling or dynamic basis, allowing them to scale with transaction volumes and participant growth.

2.3. Application & approval

> 💡 **Clear, coordinated application processes - with defined timelines and early engagement - reduce uncertainty and help NBPSPs prepare complete submissions.**

Across jurisdictions, central banks consistently highlight that uncertainty NBPSPs face in the application process as one of the main challenges. This uncertainty is typically driven by lack of clear timelines, limited transparency and fragmented communication across authorities. At the same time, central banks note that the speed and success of an application is largely driven by the maturity of the applicant, rather than the process itself.

As a result, jurisdictions that have successfully enabled access tend to:

- Publish clear application steps and expectations
- Coordinate across authorities to avoid duplication
- Encourage early engagement before formal submission

Some jurisdictions go even further and set clear timelines for applicants and for authorities. One jurisdiction communicates that the full application process typically takes between two and six months, depending on the complexity of the applicant. Another set a hard deadline of five months to complete all testing that needs to happen as part of the application process. This gives firms a realistic expectation and allows them to plan resources accordingly.

However, this is only effective when NBPSPs submit all the required information in full. This is why more advanced frameworks allow applicants to engage with authorities extensively before formally applying. This enables applicants to discuss their business model and architecture with authorities early, while they can highlight gaps before formal submission.

2.3.1. Coordination between authorities and PSOs

> 💡 **Coordinated assessments, information-sharing and regulatory reliance help prevent duplication, conflicting requirements and delays in granting NBPSPs settlement access.**

In many jurisdictions, the central bank is not the primary regulator of NBPSPs and may not even be the PSO. This creates a potential gap where the regulator assesses the firm's conduct, safeguarding and AML, while the central bank assesses settlement and liquidity risk mainly for the purposes of NBPSPs obtaining a settlement account. At the same time, the PSO examines whether a NBPSP can meet the operational and liquidity requirements.

Without coordination, this can lead to duplicate assessments, conflicting requirements and delays. Jurisdictions that have addressed this typically:

- Share information between authorities during the application process
- Rely on the primary regulator's assessment where appropriate
- Maintain regular communication on applicant progress

For example, one jurisdiction requires that the financial regulator provides a formal "non-objection" before the central bank grants access. This ensures that supervisory concerns are addressed before settlement access is approved. Similarly, another jurisdiction's pre-requisite is for a NBPSP to meet the PSO's criteria and pass its assessment first before it can come to the central bank to go through the settlement account application.

Case study: Pan-African Payment and Settlement System (PAPSS)

Expanding access to support cross-border payments and financial inclusion in Africa

The Pan-African Payment and Settlement System (PAPSS), launched by Afreximbank in collaboration with the African Union and central banks, is a cross-border payment infrastructure designed to facilitate intra-African trade by enabling payments in local currencies. A key feature of PAPSS is its inclusion of NBPSPs as direct participants, reflecting the structure of many African payment markets.

While this toolkit focuses on enabling direct access for NBPSPs to domestic payment systems, PAPSS also enables NBPSPs to connect to an international payment system. Their perspective is further demonstration for how wider access policies can contribute to the goals in the G20 Roadmap for Enhancing Cross-Border Payments.

So far, PAPSS has been rolled out across more than 21 African countries, with over 180 banks and NBPSPs onboarded or in the process of onboarding.

Policy rationale for including NBPSPs

PAPSS's decision to include NBPSPs is rooted in the unique characteristics of African financial ecosystems. In many countries, large segments of the population remain unbanked but have access to financial services through mobile money and other non-bank channels. As a result, NBPSPs often play a more prominent role in payments than traditional banks.

Allowing NBPSPs direct access to the payment system was therefore seen as essential to:

- extend cross-border payment capabilities to underserved users and SMEs
- improve access, speed and cost of intra-African payments
- enable low-value trade flows that are often not captured by traditional banking channels

Access model & impact

PAPSS enables PSPs to be either a direct participant, or an indirect participant. To be a direct participant, a PSP needs to have a settlement account with the PAPSS settlement Bank, a participant central bank, where they can settle their payments with the other participants. In addition, the recently adopted PAPSS framework will lay out a number of other criteria that a NBPSP needs to comply with before it can become a direct participant. These include:

- A minimum operational track record
- A minimum level of capital adequacy
- A customer base threshold
- Regulatory approval
- Strong governance structure

As PAPSS is an "umbrella" payment system, forming the connecting tissue between local African payment systems and central banks, the onboarding process is relatively streamlined. Participants have already gone through assessments in domestic payment systems. Therefore, the application process takes between 3-5 months.

While implementation of the NBPSP framework is still at an early stage, PAPSS expects benefits including improved access to cross-border payments, particularly for SMEs and consumers served by NBPSPs, as well as more efficient and lower-cost transactions. More broadly, the model supports the G20 Roadmap objective of improving access to payment systems as a core driver of faster, cheaper and more inclusive cross-border payments.

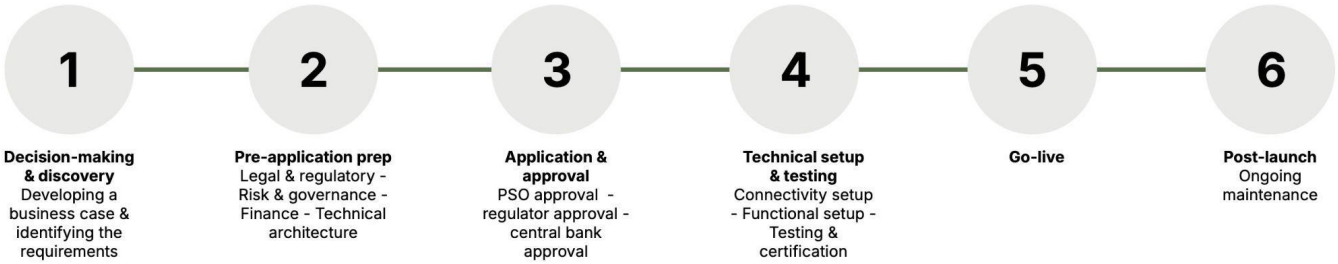
Source: PAPSS

PART 2: NON-BANK PAYMENT SERVICE PROVIDER (NBPSP) CHECKLIST TO OBTAIN DIRECT ACCESS TO PAYMENT SYSTEMS

Obtaining direct access to a payment system is a resource intensive process that requires preparation, formal application, technical integration, testing, go-live planning and ongoing compliance. Each stage requires coordination with the PSO, the regulator and/or the central bank. This checklist serves three purposes.

1. **Help NBPSPs understand the full scope of work before they apply**. Direct participation affects liquidity management, governance, risk frameworks, technical architecture, operational processes and staffing. Firms that underestimate the effort often face delays, unexpected costs or supervisory concerns late in the process.
2. **Highlight common challenges observed by NBPSPs who have gone through the process.** In many jurisdictions, payment systems were designed for bank participation. Therefore, documentation may refer to bank balance sheets, access to central bank credit or legacy infrastructure. Testing environments may be limited. Liquidity expectations may reflect conservative assumptions. Understanding these challenges early allows firms to plan properly and challenge the status quo where necessary.
3. **Identify good practices and areas where PSOs, central banks and regulators can streamline their processes based on NBPSP experiences.** Clear documentation, proportionate liquidity models, permanent test environments and transparent timelines reduce onboarding friction without weakening safeguards.

The checklist follows the typical lifecycle of a direct access project:



1. Decision-making criteria & discovery

1.1 Strategic & business rationale

✓	**Development of a clear business case for direct access.**

The first step in any direct access journey is the discovery work to build a strong business case, setting out the effort required for a direct connection. This includes evaluating aspects such as cost, control, resilience, customer experience, and liquidity efficiency. It is also important to understand staffing requirements (for participation in payment system working groups and performing operational tasks, such as funding and defunding accounts). This checklist will help NBPSPs take an informed decision based on expected costs and requirements.

A business case should encompass both the quantifiable benefits, such as whether obtaining direct access comes with a meaningful cost reduction or an increase in the speed of payments, and the more intangible benefits such as reducing reliance on a (single) sponsor bank.

A NBPSP should also assess the time it will likely take to go to market with direct participation in a payment system as opposed to going via a partner. If speed of launch is more important, then direct access may not be the preferred path. In order to get to an informed decision, NBPSPs should compare direct and indirect models.

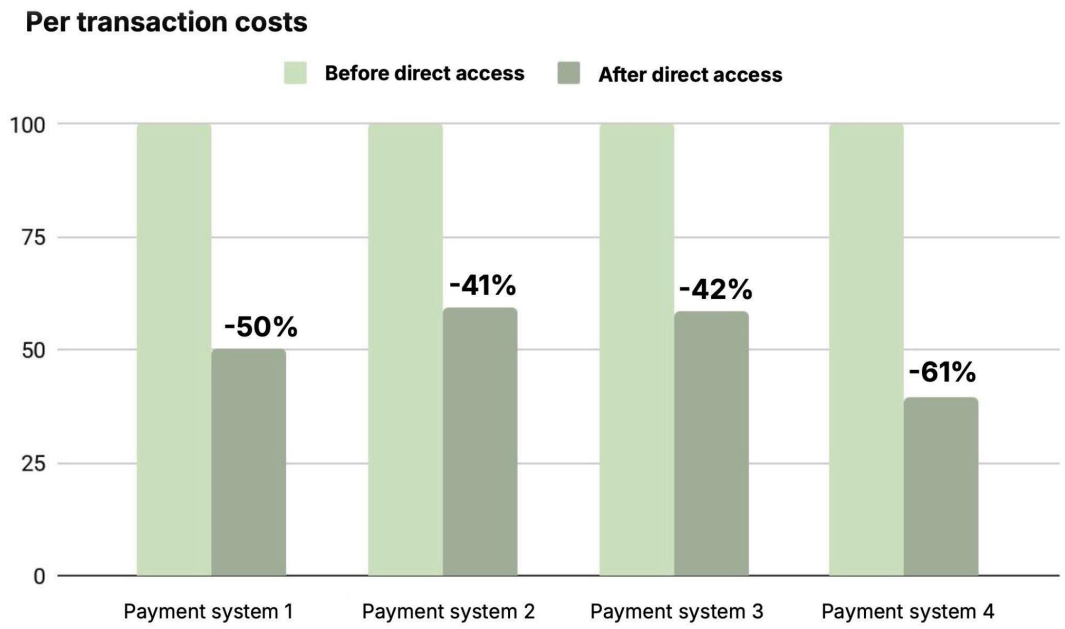
NBPSP example

One NBPSP calculated that **each direct connection** requires the following resources:

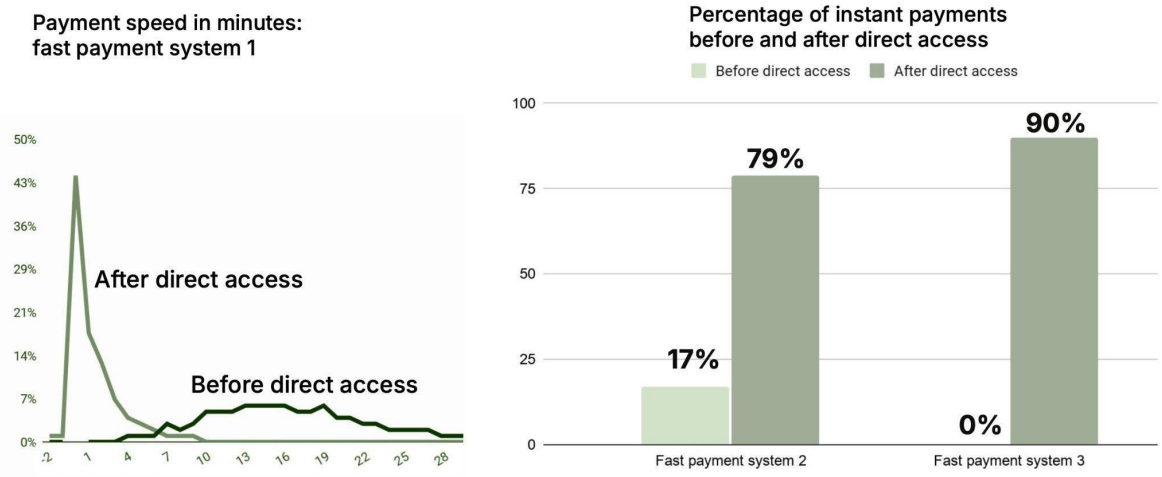
Building cost	Engineering effort	Running cost
$1 million - 1.3 million*	**20-40 engineering months**	**$50,000 - $200,000 per month**
This includes: • Infrastructure build, including engineering costs • Connectivity setup • Joining fee (if applicable): some payment systems have joining fees over > $ 1 million, so this can add up. Others have no joining fee or low joining fees (> $10,000).	This is dependent on the complexity of the direct integration. For example, if a payment system is adapted to cloud-native participants and no physical data centers are required for connectivity, the engineering effort required is much lower.	This includes requirements such as security attestations, (buddy) testing, upgrades , certificate rotation, incident handling etc. More straightforward integrations require 1 full time engineer per month, while more complex integrations require 2 or more.

** Please note that these numbers are estimates. Some direct connections are significantly cheaper or more expensive.*

The table above does not include per transaction fees, as these are highly dependent on the size and volumes processed by the recipient. However, by going direct, this NBPSP reported the following reduction in per transaction costs:



In addition, the NBPSP reported significant improvement in the speed of payments. The left-hand graph below illustrates an improvement of over 98% in crediting of the beneficiary account of the payments the NBPSP sends via one payment system (from roughly 15 minutes to instant). The right-hand graph shows that the increase of fast payments the NBPSP processes via two other payment systems, from 17% to 79% and from 0% to 90% respectively.



✓ **Comparison of direct vs. indirect/sponsor model.**

While PSPs of a certain size, scale or business model will have a stronger business case, the comparison of direct versus indirect participation is an important step to supplement the business proposal.

Direct access gives the NBPSP control, but also places full responsibility on it. In a direct settlement model, the NBPSP connects to the payment system on its own behalf. It manages its own settlement position. It must meet liquidity requirements, comply with the rulebook and, where required, operate the connection on a 24/7 basis. By contrast, in a sponsor model, a bank or existing direct participant connects to the payment system on behalf of the NBPSP. The sponsor holds the settlement account with the central bank and manages prefunding if the payment system requires this. The NBPSP relies on the sponsor's infrastructure and permissions. In this step, the NBPSP should assess whether it has the financial, operational and technical capacity to take on direct responsibility, including:

- Liquidity and capital impact: Direct participation often requires prefunding or collateral. If the NBPSP underestimates liquidity needs, it may face funding pressure on peak days. Not managing this properly can result in breaching the service level agreements (SLAs) set by the PSO or payments being rejected. In a sponsor model, the sponsor bank manages the liquidity and charges a fee for doing so. This reduces operational complexity but increases dependency.

- Infrastructure and operational burden: Direct access requires the NBPSP to build and operate the technical connection, as well as maintain it over time. This infrastructure can require hardware procurement or setting up a presence in a data centre. For example, some payment systems still require physical data centres and physical HSMs, which call for a certain level of expertise that NBPSPs may not currently possess. If a NBPSP does not already operate an infrastructure like this, it will need to hire experts or upskill existing staff. Network costs should also be taken into account. Some direct

integrations require dedicated network connection. Payment systems often demand redundancy for these connections, meaning NBPSPs have to maintain multiple connections through separate data centres or network providers to ensure continuous availability. Conversely, payment systems may only accept a selection of approved network providers, which can limit the ability to negotiate better prices. These commitments are further explored in the technical setup section (4). In a sponsor model, the sponsor typically manages most of this infrastructure, with the NBPSP connecting to the sponsor.

- Governance and ongoing commitments: Becoming a direct participant in a payment system often comes with obligations such as representation and participation in committees and working groups to contribute to any future developments within the system. While it is important that all participants have a voice in this process, it often comes with a considerable time and resources commitment. This is in addition to the resources that need to be allocated to ensure day-to-day operations, any maintenance, upgrades (whether voluntary or mandatory) and additional overlays are actioned. These commitments are set out in the maintenance and continued compliance section (6).

- Cost of remaining indirect: The NBPSP should also assess the cost of not becoming a direct participant. This cost may be non-trivial. For example, a sponsor may increase per-transaction fees as volumes grow. It may also impact a NBPSP's strategic positioning. Some payment systems restrict certain services or voting rights to direct participants.

The NBPSP should document both the benefits and the drawbacks of direct access. A structured comparison improves internal decision-making and helps supervisors understand the rationale and level of conviction for direct access.

> 💡 **PSO considerations for improvement**
> PSOs can help a NBPSP navigate this process by setting out clear guidelines, indicative pricing structure and assessment criteria, as well as timelines for application. This allows NBPSPs to make an informed decision and reduces the risk of rejected or withdrawn applications.

1.2 Payment system discovery

> ✓ **Clarification whether a settlement account at the central bank is required, optional or not permitted.**

In most jurisdictions, one of three models applies. A NBPSP can have *technical* access to a payment system (i.e. settlement still requires a sponsor), *full* access to a payment system (i.e. the NBPSP can have its own settlement account), or *indirect* access only. While a NBPSP does not carry as much of the operational burden if it does not have a settlement account, it introduces dependency on the sponsor bank and entails the risk of 'debanking', where the directly participating sponsor institution decides it will no longer provide the intermediary service. Sometimes, this can happen at very short notice, with the NBPSP facing the challenge of finding an alternative sponsor bank.

If the NBPSP can hold a settlement account, it will usually need separate approval from the central bank. This process typically includes a review of liquidity management, operational procedures and reporting capability.

In addition, NBPSPs should know the features of that settlement account. Some central banks provide access to intra-day credit and/or pay out interest on funds held on the settlement account, a feature many NBPSPs indirectly have access to via a sponsor bank. In contrast, other central banks explicitly prohibit NBPSPs from remuneration or accessing these credit facilities. A lack of access to intraday credit facilities and remuneration means liquidity may be more expensive than in a sponsor model, as NBPSPs may gain access to intraday credit or get remunerated by their sponsor, so this should feed into the business case.

One of the challenges NBPSPs face is that they may be legally eligible for settlement accounts, but the operational procedures are unclear because no NBPSP has previously applied. In these cases, approval timelines and expectations may be uncertain.

💡 **Central bank considerations for improvement**

Clear eligibility criteria and operational guidance for NBPSP settlement accounts published by central banks, including the features available to NBPSPs, enable firms to model liquidity costs accurately under each participation model.

✓ **Review of the payment system rules and technical requirements.**

A NBPSP should go through all the technical documentation that PSOs make available, so they can map every payment system requirement to internal control owners early. This includes message formats, service level agreements, fraud reporting obligations, reconciliation rules, incident notification timelines and governance participation. Early mapping supports resource planning and highlights capability gaps.

Many NBPSPs and other prospective participants face information gaps at this stage. Technical documentation is often not publicly available. Even after signing non-disclosure agreements (NDAs), information can be sparse, not readily available in English or written primarily for banks, tailored to their business model. This issue is more common in markets that have only recently opened access to NBPSPs. This leads to a much longer discovery journey and often generates serious blind spots that only become apparent once a NBPSP reaches the testing stage.

💡 **PSO & central bank considerations for improvement**

PSOs and central banks can help PSPs navigate payment system rules and technical requirements by providing complete documentation once NDAs are signed. That allows PSPs to assemble the right internal team and plan implementation realistically.

✓ **Identification of third party vendors to facilitate the connectivity and integration.**

Most direct participants in a payment system - whether banks or NBPSPs - rely on third party vendors for at least some parts of the integration. These components often include network connectivity, message exchange and transmission, HSMs, certificate management, hosting infrastructure and messaging middleware.

The NBPSP has to assess which parts of the integration they can realistically operate in-house and which require external support. Vendor selection is a strategic decision, as it affects architecture, resilience, cost, governance burden and long-term flexibility. For example, if the payment system requires message exchange over a

proprietary message queue (MQ) protocol hosted in a domestic data centre, the NBPSP may need a vendor that already operates in that environment. If the payment system requires physical HSMs, the NBPSP will have to decide whether to procure and manage them directly or use a managed service provider, which comes at an additional cost. However, it is worth noting that payment systems, regulators or central banks may only have a small number of "approved" providers to choose from, which can limit the NBPSP's options.

⚠ Five common vendor-related challenges

1. **Bank-centric documentation:** vendor documentation can at times assume bank knowledge (e.g. familiarity with local proprietary messages formats) or bank infrastructure. NBPSPs without prior exposure to those systems often require additional consulting support to interpret requirements.
2. **Vendor lock-in risk:** this is especially true for connectivity vendors, which can become deeply embedded in a NBPSP's architecture. Switching vendors later may require full recertification with the payment system or a redesign of message flows.
3. **Evolving requirements:** payment systems change over time, introducing stricter service levels or new overlays, and vendors need to be able to scale and adapt. For example, a new name-checking service may require a response within one second. If the vendor cannot meet this requirement, the NBPSP becomes non-compliant even if its internal systems are capable.
4. **Underestimated maintenance effort:** vendors may require regular certificate renewals, security attestations, middleware upgrades and mandatory regression testing. These recurring tasks require operational planning and budget.
5. **Hardware procurement can create delays:** for example, physical HSMs may have long delivery times. Installation may require on-site visits in specific data centres. This can extend onboarding timelines by several months.

💡 **PSO & regulatory considerations for improvement**

PSOs can support NBPSPs by ensuring their connectivity models do not create unnecessary barriers to entry for certain types of participants. They could consider clearly describing acceptable connectivity models and avoiding unnecessarily prescriptive hardware requirements where security objectives can be met through certified cloud-based alternatives. PSOs are encouraged to provide clear certification requirements so that vendors and NBPSPs understand performance expectations in advance.

Authorities' adoption of proportionate outsourcing expectations that recognise well-managed, industry-standard connectivity components need not increase systemic risk, can support NBPSPs. Clear, technology-neutral requirements can reduce onboarding friction and support innovation without compromising resilience.

2. Pre-application checklist

Once the NBPSP has completed its strategic assessment and discovery work, it should prepare for formal application. The pre-application phase determines whether the application proceeds smoothly or becomes delayed by supervisory questions, missing documentation or late design changes. Early engagement with regulators, PSOs and the central bank reduces uncertainty and avoids rework during the formal approval phase.

At this stage, NBPSPs have to demonstrate that they understand the operational, legal and financial implications of direct participation. They should update their risk policies, safeguarding framework, incident response

procedures and board reporting to reflect that the firm will now manage its own settlement position and comply directly with payment system rules.[12]

The pre-application stage usually covers:



2.1 Legal & regulatory preparation

✓	**Confirmation of the correct regulatory licence and permissions.**

In most jurisdictions, eligibility for direct access depends on licence type. While this is a relatively straightforward requirement, NBPSPs have experienced issues even when they are formally eligible. For example, electronic money institutions/issuers or payment institutions may be eligible in law, but the supervisory authority may not yet have assessed a non-bank as a direct participant in practice. This can create friction and differences in interpretation.

That friction is common where safeguarding requirements intersect with prefunding obligations. NBPSPs typically have to safeguard customer funds to protect them from insolvency and misuse. However, payment systems often require those same funds to be mobilised operationally, for example by placing them into a settlement account or collateral pool. Supervisors may question whether those funds remain properly safeguarded under insolvency rules. That uncertainty over whether settlement balances qualify as safeguarded funds can delay applications significantly.

NBPSPs should engage with their regulator early and request written confirmation that prefunding and settlement arrangements comply with safeguarding rules. They should prepare a short legal analysis explaining how customer funds are protected in the settlement model, and ensure that their safeguarding policy explicitly references payment system participation.

2.2 Governance & risk framework

Direct access requires the NBPSP to treat payment system participation as a critical activity, not just an operational function. It comes with explicit risk ownership, resilience testing, and independent assurance.

✓	**Documentation of the risk management and operational resilience frameworks specifically for payment system participation.**

[12] For the purposes of this document, a (payment scheme) means the governed set of rules, standards and operational arrangements for providing a particular payment service. It is usually documented through a rulebook, technical specifications and participant procedures. A payment scheme may form part of a wider payment system and is not necessarily maintained by a separate organisation or infrastructure.

While any regulated NBPSP will have risk management and operational resilience frameworks in place, PSOs, regulators and central banks require frameworks beyond generic enterprise risk policies. NBPSPs have to ensure that their risk framework explicitly covers direct payment system participation.

Therefore, they should include payment system participation as a distinct risk category in their risk taxonomy. It should set out a clear risk appetite for areas such as settlement exposure, liquidity shortfalls and payment system rule breaches. NBPSPs have to identify and document all critical dependencies related to payment system participation. This includes connectivity providers, HSMs, cloud infrastructure, treasury processes and incident reporting channels.

In order to do this, they should conduct scenario testing that reflects realistic payment system-related risks. For example, a NBPSP should test how they would respond if inbound settlement funds were delayed for several hours while outbound payments continued. Or how they would react to a temporary loss of connectivity to the payment system. For each scenario, there should be clear escalation procedures, specifying the responsible team, decision-making authority and communication steps. These procedures should be documented, understood and tested by relevant staff.

Supervisors will expect evidence that the firm can continue operating safely during stress events without creating contagion risk to the payment system. A documented and tested resilience framework demonstrates that capability.

✓ **Creation of an incident response policy for payment system participation.**

Most payment systems expect an immediate notification for certain types of incidents. NBPSPs should identify which incidents require notification under the payment system rulebook, comparing the rulebook's definition of a "major participant incident" to their own internal severity classifications. These definitions are often not identical. An incident that the firm classifies as "high severity" may not meet the payment system threshold, and an incident that the PSO considers reportable may not trigger internal escalation automatically. Reconciling these definitions and documenting clear notification triggers is key.

In addition, NBPSPs should prepare structured post-incident reporting templates in advance. Payment systems typically require a clear description of the incident, the time of occurrence, the number of impacted transactions, a root cause analysis and a description of remediation steps. If these templates are not prepared in advance, teams end up having to draft them under operational pressure during a live incident.

It is good practice to include a payment system-specific annex within a NBPSP's existing incident response policy. This annex should set out payment system notification triggers, named escalation contacts, reporting timelines and communication channels. Some NBPSPs discover during onboarding that their internal incident definitions do not align with payment system reporting thresholds. This misalignment can result in delayed notifications and rulebook breaches. Other firms lack a clearly defined escalation chain, which creates confusion during live incidents.

💡 **PSO & regulatory considerations for improvement**

Publication of precise definitions of reportable incidents and standard reporting templates by PSOs can help applicants. Proportionate and operationally realistic reporting requirements from regulators as well as clear definitions and structured templates reduce the risk of avoidable breaches.

✓ **Establishment of an outsourcing framework for dependencies related to direct payment system participation (cloud or third-party dependencies).**

Direct participation in a payment system usually involves reliance on third parties. These third parties may include cloud providers, network providers, connectivity vendors or managed hardware providers. Regulators and PSOs will assess whether these dependencies introduce operational, concentration or systemic risk. The NBPSP should therefore establish a clear outsourcing framework before submitting its application.

Where a NBPSP relies on a third party to operate or manage its technical connection to a payment system, it should assess whether the arrangement constitutes outsourcing under the applicable regulatory framework. Where it does, it should assess whether the outsourced service is important, particularly if its disruption would materially impair the NBPSP's ability to send, receive or settle payments. Furthermore, it should assess whether these arrangements qualify as critical outsourcing under applicable regulatory guidelines (e.g. European Banking Authority's outsourcing guidelines, Monetary Authority of Singapore's outsourcing expectations).

Some NBPSPs treat connectivity providers as technical suppliers rather than critical service providers. This approach can create gaps in documentation and oversight. For example, the firm may not define how it would continue operating if the connectivity provider experienced an outage. It may not test failover arrangements. It may not ensure that audit rights are included in the contract. These gaps often become visible during supervisory review. In other cases, firms cannot demonstrate how they would replace a vendor or migrate connectivity if necessary. These weaknesses often surface during supervisory review and delay approval.

💡 **Regulatory considerations for improvement**

It is helpful when regulators provide clear guidance on how outsourcing rules apply to payment system connectivity and recognise that many cloud and connectivity providers operate under established regulatory and security standards. Many cloud providers have developed security, resilience, audit and operational capabilities comparable to those of established data centre and technology infrastructure providers. Cloud services can therefore be assessed on the risks and critical functions they support, rather than treated as inherently less suitable because of the technology or hosting model used. When PSOs align their resilience requirements with regulatory outsourcing expectations, they avoid duplication or conflicting obligations. For example, where a regulator permits multi-region cloud deployment subject to resilience testing and audit rights, a payment system does not simultaneously require single-location domestic hosting unless it can clearly justify the additional risk mitigation.

2.3 Financial requirements

Direct participation means the NBPSP manages its own settlement risk. It may need to prefund a settlement account, post collateral or contribute to loss-sharing arrangements. These requirements affect liquidity, working capital and, in some cases, regulatory buffers. The NBPSP has to assess this impact in detail before applying.

✓ **Preparation of a capital impact assessment.**

NBPSPs exploring direct access should prepare a capital impact assessment. This document sets out the current regulatory capital position, the existing capital buffers above minimum requirements, and the amount of

prefunding required at go-live. As part of the memo, NBPSPs should also look into the impact of tying up liquidity in settlement accounts. Supervisors and PSOs will expect the NBPSP to demonstrate how it will manage that impact. They will look for mitigants such as committed credit lines, internal liquidity buffers, or a short-term fallback arrangement with a sponsor bank.

✓	**Development of a liquidity plan for prefunding / settlement.**

Many payment systems use deferred net settlement, which means that payment instructions may be executed to counterparties before incoming customer funds or other participants' funds settle. This creates a liquidity risk.

For example, the NBPSP may send 100 million in outbound payments during the morning cycle. If inbound funds are delayed because of payment system latency or connectivity disruption, the NBPSP has to find a way to fund the gap until settlement completes. To mitigate this, NBPSPs should calculate worst-case intraday exposure and model scenarios such as peak transaction days, payment system outages, delayed inbound settlement or market shocks.

NBPSPs report challenges in systems where settlement funding requires manual action during fixed time windows. Those manual processes are more prone to operational errors. Missing a window can leave the NBPSP exposed for several hours. Central banks can help avoid this, by modernising funding interfaces and reducing reliance on manual processes.

In addition, NBPSPs should carefully assess how settlement accounts can be funded in practice, as this can create hidden liquidity constraints. In some (fast) payment systems, prefunding is only possible via specific rails such as the RTGS system, which may not be accessible to NBPSPs or have limited operating hours. This means that participants cannot add liquidity to their settlement accounts at all times and have to forecast expected payment volumes outside those hours and prefund accordingly. This creates additional forecasting risk and can lead to higher precautionary buffers, particularly for NBPSPs with less predictable payment flows. Central banks and PSOs can mitigate this by enabling more flexible or extended funding mechanisms that better align with 24/7 payment systems.

One of the main issues NBPSPs face is around liquidity efficiency and prefunding expectations. Some payment systems require participants - and NBPSPs in particular - to maintain conservative prefunded balances to ensure that settlement obligations can always be met. This can create significant liquidity costs for NBPSPs, as liquidity is not a plentiful resource for most NBPSPs. Funds held in prefunded settlement accounts are often ring-fenced and cannot be used for operational purposes. In addition, some central banks do not remunerate balances held by NBPSPs. That means that prefunding requirements can tie up large amounts of cash that generate no return.

For large banks, holding sizeable liquidity buffers is often part of normal balance sheet management. Banks may also have access to central bank credit facilities and much larger internal liquidity pools. For newer players or leaner PSPs, however, tying up large buffers can have a direct impact on business growth and profitability.

In practice, some payment systems apply conservative prefunding requirements because participants cannot see their settlement position in real time due to the lack of real-time tracking. If settlement positions are only updated periodically or through batch reports, participants have to hold additional buffers to avoid the risk of breaching settlement obligations. This is much more problematic for smaller or leaner PSPs than for larger incumbents. Large banks often hold larger liquidity buffers than required because liquidity is easier for them to obtain and manage.

💡 **PSO and central bank considerations for improvement**

PSOs and central banks can improve liquidity efficiency by providing participants with accurate, near real-time reporting of settlement positions and available balances in settlement accounts. If participants can track their settlement exposure continuously, they can manage liquidity more precisely and reduce the need for large precautionary buffers. This also allows the PSO to set lower default buffers without creating any settlement risk. Real-time visibility also improves reconciliation and reduces operational risk during incidents. Reducing unnecessary liquidity buffers does not weaken resilience. Instead, it allows participants to manage risk based on accurate information rather than conservative assumptions. This frees up liquidity to grow and scale the business instead.

2.4 Technical architecture readiness

Direct participation requires the NBPSP to build and operate a technical connection to the payment system. Before submitting an application, the NBPSP must decide how that connection will be implemented and whether its internal systems are capable of supporting payment system requirements.

This phase focuses on architectural decisions that will affect the entire lifecycle of the connection, including operational resilience, incident management and long-term maintenance.

✓ **Definition of the integration and connectivity design (direct messaging, gateway provider).**

This is one of the most consequential design choices when pursuing a direct connection. A NBPSP should figure out which connectivity options a payment system allows and which route it would like to pursue. Generally, there are two options:

1. Direct connectivity (in-house integration): a PSP builds and operates its own secure network connection to the payment system, communicating directly with the PSO's endpoint. This approach requires the NBPSP to operate and maintain several components itself. These often include network connections, message transport protocols, certificate management and cryptographic key storage. In some systems, keys must be stored in HSMs. These may be physical devices installed in a data centre or cloud-based HSM services, depending on payment system requirements.

   Direct connectivity gives the NBPSP full control over its infrastructure. It usually provides the best visibility during incidents because engineers can see payment system responses directly rather than through an intermediary. It also tends to have the lowest marginal cost once the integration is fully operational. However, direct integration requires significant engineering investment and ongoing operational support. The NBPSP has to maintain 24/7 monitoring, certificate management processes and incident response procedures.

   In addition, the NBPSP has to adapt to legacy infrastructure requirements that are outside its control. For example, some payment systems require leased network lines, physical presence in specific domestic data centres or proprietary messaging middleware.

2. Gateway provider connectivity: under a gateway model, the NBPSP connects to the payment system through a specialised third-party provider. The gateway provider maintains the direct payment system

connection and provides it to the NBPSP through an API or managed interface. This model reduces the initial engineering burden. The gateway provider typically manages certificate rotation, network connectivity and message transport. For example, a gateway provider may operate the message queue (MQ) infrastructure required by the payment system and provide it to the NBPSP through a Representational State Transfer application programming interface (REST API).

However, gateway models introduce different risks. The NBPSP may have less visibility during incidents because it can only see gateway errors rather than payment system-level errors. This can complicate troubleshooting and incident reporting because they cannot see the root cause. Gateway models can also create concentration risk. If many PSPs rely on the same gateway provider, an outage at that provider may affect multiple participants simultaneously.

When selecting an integration model, NBPSPs should consider several factors. These include expected transaction volumes over the next three to five years, internal engineering capability, treasury operations, regulatory outsourcing requirements, operational resilience expectations, time-to-market objectives and the long-term cost structure of the integration. For example, a NBPSP expecting to process high volumes over the next few years may prefer direct connectivity because it reduces long-term dependency on a third party. A smaller firm entering a new market may choose a gateway solution to reduce implementation time or to gain operational experience before building its own direct connection.

In addition to architectural preferences, the chosen integration design has to be able to meet the payment system's performance and resilience requirements. These are typically defined in the payment system rulebook and are not optional. Two dimensions are particularly important:

- **Volume capacity**: the setup has to be able to process expected transaction volumes, including peak days and future growth. This depends on the NBPSP's business model and scaling assumptions.
- **Latency / response times**: the setup has to meet strict timing requirements defined by the payment system. This is especially critical for FPS, where participants may be required to respond within a few seconds (or less for certain overlay services such as confirmation of payee).

These requirements can directly influence the choice of integration model. For example, gateway-based models may introduce additional network hops or processing layers that increase latency, while direct integrations may provide tighter control over performance optimisation.

Availability and reliability requirements should also be factored into the integration design from the outset. Many payment systems operate on a 24/7/365 basis with minimal maintenance windows (or no windows at all to allow for continuous maintenance). Participants are expected to meet strict uptime targets and demonstrate robust disaster recovery capabilities. This typically includes defined targets for detection and recovery and clear recovery objectives. NBPSPs should ensure that their chosen architecture (including any third-party providers) can meet these expectations in practice, not only in theory.

> 💡 **PSO considerations for improvement**
> PSOs can help NBPSPs navigate this process more easily by clearly describing all available connectivity options, their technical requirements and performance SLAs. Providing architecture guidelines and example reference implementations can help new participants make informed decisions. They should avoid steering NBPSPs toward a specific model unless there is a clear operational justification.

✓ **Ensuring payment messaging and payment flow readiness.**

Although many payment systems now use the ISO 20022 messaging standard, there are many local variations of the standard and proprietary message formats are still in use too. When NBPSPs build their own direct connection, they should map their payments against all the possible paths (and therefore all possible codes), including unhappy paths, and test for these hundreds of scenarios. For example, the NBPSP must define how its systems will process payment confirmations, payment rejections, returns and reversals, enquiry messages and fraud notifications. Each of these scenarios typically corresponds to specific message codes and response formats.

Many payment systems document successful payment flows clearly but provide limited guidance on failure scenarios. NBPSPs frequently discover edge cases during testing, or occasionally even after go-live. For example, they may encounter unexpected rejection codes or timeout behaviours that were not clearly documented. Where documentation is incomplete, engineers may need to interpret message behaviour through trial and error during testing. Some payment systems have over 2000 pages worth of documentation, setting out the various paths with the relevant codes and messaging. In contrast, other payment systems only provide 20-30 pages and leave a lot of areas open to interpretation. In addition, this documentation is often only available once an applicant has made a commitment to join the payment system, which greatly reduces the readiness of the NBPSP because they were unable to fully scope the preparatory work. It would be preferable to make the documentation available under NDA when the NBPSP is exploring their options, so they are more informed about the right path to take.

💡 **PSO considerations for improvement**

PSOs can significantly reduce onboarding time by providing comprehensive message documentation, including example messages, full code lists and clearly defined unhappy path scenarios. This reduces interpretation risk and ensures that all participants implement the payment system consistently. It is also particularly helpful if PSOs make a high-quality testing environment available and ensure it is reflective of the environment a NBPSP will face in production.

2.5 Discovery questionnaires

Discovery questionnaires are often perceived as administrative formalities. In practice, they are a key stage in the pre-application process. PSOs, regulators and central banks use these questionnaires to assess whether an applicant understands the operational and financial responsibilities of direct participation. The quality and completeness of the responses strongly influence how authorities assess the NBPSP's readiness. Discovery questionnaires should therefore be treated as structured due diligence exercises rather than simple information requests. Well-prepared responses can significantly reduce the number of follow-up questions and shorten the application timeline.

✓ **Completion of the PSO due diligence questionnaire.**

PSOs typically require detailed information about the NBPSP's governance, risk management framework, operational resilience, liquidity management and cyber security controls. Although the exact format varies across jurisdictions, most questionnaires aim to answer two core questions. First, can the NBPSP comply with the operational and technical requirements of the rulebook? Second, does the NBPSP introduce operational or systemic risk to the payment system? Therefore, the responses have to go beyond high-level descriptions. PSOs

usually expect evidence-based answers supported by data, internal policies, monitoring metrics and stress-testing results.

The most common challenge is that many questionnaires were originally designed for banks and PSO approvers often have limited precedent assessing NBPSPs. Templates may assume that the applicant has access to central bank credit facilities, large balance sheet buffers or legacy infrastructure. For example, some NBPSPs report being asked to justify why they do not rely on intraday credit or why they operate a cloud-based architecture instead of hosting systems in physical data centres. In these cases, NBPSPs often need to explain how alternative controls achieve the same risk mitigation. For instance, real-time liquidity monitoring and automated payment throttling (i.e. slowing or temporarily limiting outgoing payments when liquidity becomes tight) can provide similar safeguards to bank-style liquidity buffers.

Where non-bank participation is new, PSOs may initially request conservative liquidity buffers (see 2.3) or infrastructure controls. Once the NBPSP demonstrates detailed monitoring tools and stress testing capabilities, these expectations are often recalibrated. In some cases, the first non-bank participant effectively sets a precedent. For example, some payment systems initially assumed that participants would host infrastructure in physical data centres. After the first NBPSP demonstrated the resilience and security of its cloud architecture, those expectations were revised and cloud connectivity became accepted practice.

✓ **Completion of the central bank risk questionnaire (if required).**

If direct participation includes access to a settlement account, the central bank may require a separate risk questionnaire. These questionnaires usually focus on liquidity management, operational resilience and settlement risk. Central banks often ask applicants to demonstrate how they will manage peak settlement exposure and how they will respond to stress scenarios. For example, the NBPSP may be asked to model how it would manage a day in which outbound payments exceed inbound payments by a significant margin. The central bank can also request stress testing that assumes delayed inbound settlement flows or temporary loss of connectivity to the payment system.

In jurisdictions where non-bank settlement participation is new, central banks may initially apply supervisory expectations designed for banks. This can lead to requests for buffers or collateral arrangements that do not fully reflect the business model of NBPSPs. Another common challenge arises when central banks rely on manual operational processes for settlement account funding or reporting. These processes can create additional operational complexity for new participants, especially because NBPSPs tend to rely much more on automation than incumbents.

✓ **Completion the self-assessment against payment system rulebooks.**

Many payment systems require applicants to formally attest that they comply with the payment system rulebook. Even when this is not mandatory, conducting an internal self-assessment is an important preparation step to eliminate surprises later on. Payment system rulebooks often contain detailed operational obligations. These may include requirements for message handling, cut-off times, dispute resolution procedures, incident reporting timelines, fraud monitoring and participation in governance forums.

💡 **PSO considerations for improvement**

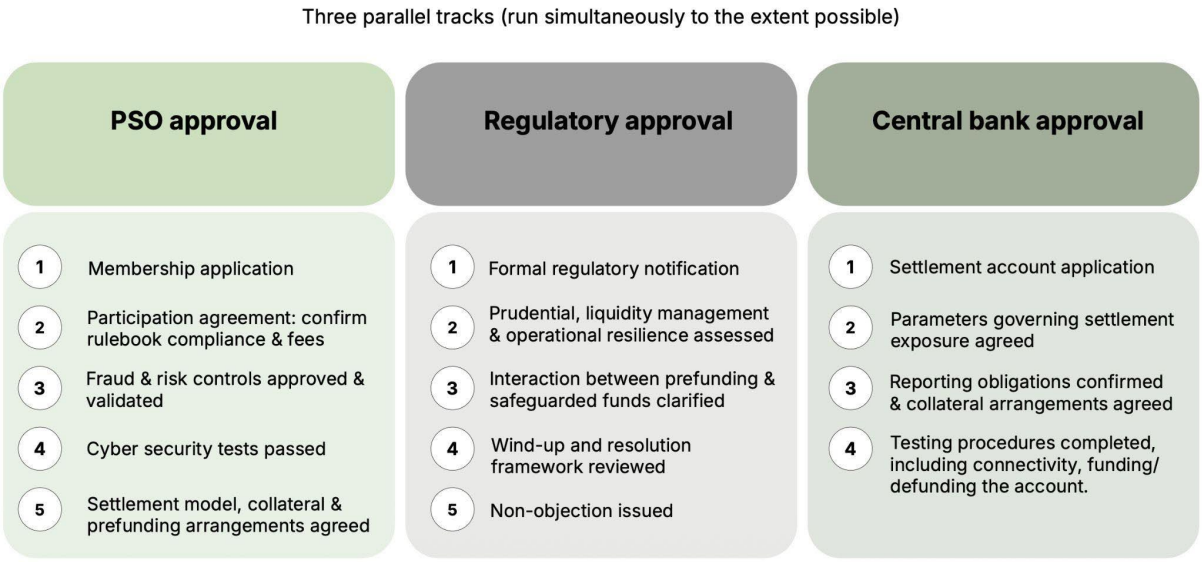
PSOs can make onboarding more predictable by consolidating operational obligations into clearly structured documentation and participant guidance. Rulebooks should clearly identify mandatory participant

responsibilities and separate them from background information. Providing implementation guides or onboarding checklists for new participants can also significantly reduce discovery time and improve consistency across participants.

3. Application & approval checklist

Once discovery and pre-application preparation are complete, the NBPSP enters the formal application phase. At this stage, the focus shifts from exploration to verification. The NBPSP has to demonstrate that the controls described during discovery are already implemented, tested and operational.

From the perspective of the authorities, this phase is less about introducing new requirements and more about confirming that the NBPSP can operate safely as participant of the payment system.



As these processes often run simultaneously, coordination between the relevant authorities can significantly reduce onboarding delays. In some jurisdictions, the PSO, regulator and central bank actively coordinate their reviews. In others, the NBPSP has to manage communication between the different stakeholders itself. Where coordination channels are weak or unclear, the approval process can become fragmented and significantly longer. Some of the requirements can also be contradictory if there is little to no coordination between stakeholders. Authorities can reduce this friction by establishing structured coordination channels between supervisors, PSOs and central banks during participant onboarding.

3.1 PSO approval

During this phase, the PSO evaluates whether the NBPSP can operate safely and reliably as a participant within the payment system. While eligibility may already have been confirmed during discovery, the PSO must now verify that the NBPSP can meet the operational, technical and governance requirements of the rulebook, without creating risks for other participants. The PSO review focuses predominantly on operational readiness. It examines whether the NBPSP can process transactions correctly, manage settlement obligations and respond appropriately to operational incidents.

This assessment differs from the regulatory review, where the focus is on firm-level risks such as safeguarding, governance, risk management and capital adequacy. The PSO focuses on operational behaviour within the payment system. Although these reviews cover related topics, they address different questions. As a result, approval by the PSO does not automatically satisfy the regulator and vice versa.

PSO approval and regulatory approval usually proceed in parallel. Misalignment between payment system participation requirements and supervisory expectations can delay onboarding. This situation often occurs in

jurisdictions where non-bank direct participation is relatively new and payment system documentation still reflects bank-only participation models.

3.1.1 Participation application

✓	**Submission of direct participant application.**

The application pack requirements vary by jurisdiction. They typically include corporate documentation such as certificates of incorporation, regulatory licences, ownership structure and board approval of the participation decision. PSOs also request information on governance structures, financial position, technical integration plans and operational readiness. Some application forms may still contain bank-specific language. However, these issues are usually identified and clarified during the discovery phase.

3.1.2 Participation agreement

✓	**Signing of the participation agreement and confirm rulebook compliance.**

The participation agreement is a contractual relationship between the NBPSP and the PSO. It typically incorporates the payment system rulebook(s) dynamically. This means that the participant agrees not only to comply with the current version of the rulebook, but also with future amendments introduced by the PSO. In practice, this creates ongoing implementation obligations. Participants have to continuously monitor payment system updates and plan engineering capacity for mandatory upgrades. For example, payment systems may introduce confirmation-of-payee or name-checking services, request-to-pay overlays, updated ISO 20022 message versions, or stricter response time requirements for fast payments. Participants have to implement these changes even if they require system upgrades or architectural adjustments. For NBPSPs, this highlights the importance of active participation in payment system governance forums. Payment system working groups and technical committees often define upcoming changes before they become mandatory. Participation allows NBPSPs to understand upcoming requirements early and ensure that new rules are proportionate for non-bank participants. It allows them to help shape new requirements and capabilities, as well as changes to payment system rules.

The participation agreement generally confirms that the NBPSP meets the eligibility criteria, holds the required regulatory licence, complies with applicable laws and regulations, and has sufficient operational capability, governance arrangements and liquidity to participate safely in the payment system.

It will also set out settlement and funding obligations (e.g. prefunding, collateral or guarantee fund contributions), liability and indemnity provisions, operational standards, and grounds for suspension and termination, including regulatory action or failure to meet settlement obligations.

✓	**Agreement on payment system fees and associated fees.**

Direct participation usually involves several categories of fees beyond transaction processing charges. Participants may need to pay onboarding fees, annual membership or participation fees, testing and certification fees, connectivity fees or fees related to overlay services. Fee structures sometimes differ depending on the participant category. For example, direct settlement participants may face different charges than participants with technical access. Some payment systems were originally designed for large PSPs processing very high volumes. As a result, minimum fee thresholds or fixed participation costs can represent a higher relative burden

for smaller NBPSPs during the early stages of participation. In addition to formal payment system fees, NBPSPs have to consider indirect costs. These may include infrastructure investments, governance participation, mandatory system upgrades and ongoing compliance obligations.

> 💡 **PSO considerations for improvement**
> PSOs can improve transparency by publishing comprehensive fee schedules, participant categories and cost structures. Clear fee disclosures allow applicants to assess the full economic impact of direct participation before committing to the application process.

3.1.3 Fraud & risk controls

✓ **Review and approval of fraud controls.**

PSOs require participants to maintain strong fraud prevention controls. Fraud incidents can affect the reputation of the payment system and undermine trust between participants. Some payment systems define fraud performance benchmarks or require participants to contribute to shared fraud reporting platforms. A common challenge is that payment system-level fraud tools and data-sharing arrangements may have been built around direct bank participants. As a result, NBPSPs may find that they cannot access the same fraud intelligence tools on the same basis as incumbent banks, or that the operational process for NBPSPs is unclear.

> 💡 **PSO & authorities considerations for improvement**
> PSOs should also make the fraud performance metrics used to assess participant behaviour available to participants. These metrics may include thresholds for fraud rates, reporting timelines or reimbursement obligations. Participants should know in advance how these metrics are calculated and how they affect payment system compliance. Transparent definitions reduce the risk of disputes and ensure that all participants operate under the same expectations. Authorities can support this by encouraging the development of shared fraud intelligence utilities that are accessible to all regulated participants. As highlighted, in some markets, fraud monitoring tools have historically been built around bank-only participation models. As access expands to NBPSPs, these frameworks may need to be updated to ensure that new participants can both contribute data and benefit from shared intelligence.
>
> Finally, harmonised fraud reporting formats and interfaces across payment systems could help reduce operational burdens, where feasible. Many NBPSPs participate in multiple payment systems. If each payment system requires a different reporting structure or data format, the operational burden increases without necessarily improving fraud detection.

✓ **Validation of operational risk controls.**

Operational risk validation focuses on whether the NBPSP can reliably process, reconcile and monitor transactions within payment system rules. The PSO typically examines how the NBPSP processes incoming and outgoing payments, manages settlement balances, reconciles transactions and handles operational incidents.

One of the most common issues identified during payment system certification is insufficient automation in reconciliation processes. Some NBPSPs initially rely on manual reconciliation between payment system reports and internal records. This approach quickly becomes unsustainable once transaction volumes increase. Another

common challenge arises when NBPSPs do not fully implement error and exception handling scenarios. Many payment systems document successful payment flows clearly, but provide limited guidance on failure cases. As a result of this incomplete documentation, some participants only discover missing logic during certification testing.

> 💡 **PSO considerations for improvement**
> PSOs can improve operational resilience by providing clear documentation of failure scenarios.

NBPSPs also report reconciliation challenges when the timing, level of detail or structure of the payment system reporting formats differ from the records maintained in the NBPSP's own systems. For example, some payment systems report transactions in batch settlement files while the participant's internal ledger operates in real time and reports every payment individually. These reconciliation requirements should be addressed early in the design of the NBPSP's systems.

3.1.4 Cyber security framework

✓	**Review of cyber security framework.**

PSOs typically require participants to demonstrate that their systems meet defined cyber security standards before granting access to the payment system. The purpose of this review is to ensure that the participant's infrastructure cannot be used as an entry point to compromise the payment system or other participants.

One of the most common challenges for NBPSPs is that some payment systems maintain bespoke cyber security certification frameworks that differ from widely used industry standards. For example, a NBPSP may already hold an ISO 27001 certification, demonstrating that it operates an independently assessed information security management system, or have a SOC 2 assurance report assessing the design and operating effectiveness of its security and resilience controls. However, the payment system may still require additional documentation or testing specific to the participant's connection to its infrastructure, despite existing and universally accepted assurances. This makes the cyber reviews more cumbersome and less streamlined.

> 💡 **PSO considerations for improvement**
> PSOs can reduce friction by aligning their requirements with widely recognised industry standards. For example, the NIST Cybersecurity Framework can provide a common structure for assessing cyber risk governance, asset and dependency identification, protective controls, detection capabilities, incident response and recovery. As the NIST framework is outcome-based rather than prescriptive, it can be applied consistently to banks and NBPSPs while allowing participants to use different technologies and architectures to achieve equivalent security outcomes.
>
> Where possible, existing certifications such as ISO 27001 or SOC 2 could be accepted as evidence of baseline security controls. Where Swift forms part of the participant's connectivity or messaging environment, the participant should also demonstrate compliance with the applicable requirements of the Swift Customer Security Programme and its Customer Security Controls Framework, including the relevant attestation and independent-assessment requirements. Additional payment system-specific testing should focus only on elements that are unique to the payment system.

Another recurring issue arises when payment systems were designed around participants with on-premise core banking systems. Some PSOs historically assumed that participants would host systems in physical data centres with dedicated network appliances. Cloud-native NBPSPs may therefore need to explain how cloud security controls provide equivalent or stronger protection. For example, an NBPSP may rely on cloud-based key management services or cloud HSMs rather than physical devices installed in a data centre. Similarly, infrastructure may be deployed across multiple cloud regions rather than a single physical site.

💡 **Regulatory & central bank considerations for improvement**

Regulators and central banks can support consistent cyber security expectations across payment systems by promoting common security frameworks and standards. Encouraging alignment between supervisory cyber security requirements and payment system-level certification processes reduces duplication and simplifies compliance for participants operating across multiple payment systems.

3.1.5 Liquidity arrangements

✓ **Confirmation of the settlement model (prefunding vs. deferred net settlement vs. RTGS).**

The PSO will confirm the settlement structure under which the NBPSP participates. Although settlement arrangements are also discussed during the discovery phase, they may be reassessed during formal approval. This can happen when authorities examine the NBPSP's liquidity monitoring tools or reassess stress scenarios. For example, if a participant cannot demonstrate real-time visibility of its liquidity position, the PSO may require larger prefunding buffers to reduce the risk of settlement shortfalls.

Another common challenge occurs when payment system settlement reporting is not provided in real time. If participants receive settlement reports only periodically or in batch files, they may need to maintain larger precautionary liquidity buffers to avoid breaching settlement obligations, which comes at a high cost.

💡 **PSO considerations for improvement**

PSOs can support more efficient liquidity management by providing participants with accurate and timely visibility of their liquidity position.

✓ **Finalisation of collateral or prefunding arrangements (if applicable).**

As part of the approval process, the NBPSP and the PSO must agree on the final prefunding or collateral arrangements. These arrangements may include maintaining minimum prefunded balances, posting collateral to cover settlement exposure or contributing to payment system-level guarantee funds. Although these requirements are usually discussed during discovery and pre-application preparation, details may still change during formal approval.

NBPSPs report that prefunding requirements can change late in the onboarding process. This may occur when additional stakeholders become involved or when new stress scenarios are introduced during review. In some cases, PSOs initially assume conservative liquidity buffers. Once the NBPSP demonstrates detailed monitoring tools and automated liquidity controls, those expectations may be recalibrated.

Another common challenge arises when collateral models assume that participants hold certain types of financial assets (e.g. government bonds, central bank eligible securities or other high-quality liquid assets). Banks commonly hold these instruments as part of their liquidity management and regulatory requirements. NBPSPs, however, often operate under different balance sheet structures. Their assets may primarily consist of safeguarded customer funds held in commercial bank accounts rather than securities portfolios. As a result, they may not hold the types of financial instruments required by traditional collateral frameworks. In these cases, the NBPSP may need to negotiate alternative collateral arrangements, such as cash collateral held in a designated account or guarantees provided by a sponsor bank.

💡 **PSO & central bank considerations for improvement**

PSOs and central banks can reduce friction by recognising that different participant types have different balance sheet structures and reflecting that in arrangements.

3.2 Regulatory approval

In parallel with the PSO review, the NBPSP has to obtain approval or non-objection from its financial regulator to participate directly in the payment system. The purpose of the regulatory review is to assess whether direct participation materially changes the risk profile of the NBPSP and whether the firm can manage those risks safely.

Regulators typically focus on prudential, operational and consumer protection considerations, while the PSO is primarily concerned with payment system integrity and operational capability. For example, regulators will examine how direct participation affects safeguarding arrangements, liquidity management, operational resilience and the firm's ability to continue operating during stress events. Regulators will typically rely on information provided by both the NBPSP and the PSO when forming their assessment.

✓ **Submission of a formal regulatory notification or permission request.**

In many jurisdictions, direct participation in a payment system requires a formal regulatory notification or a variation of the NBPSP's existing licence. For example, the regulator may require the NBPSP to notify them that it intends to become a direct participant in a payment system or to obtain confirmation that this activity falls within its existing permissions. The exact process varies across jurisdictions. Some regulators foresee a formal approval process, while others issue a "non-objection" letter confirming that the regulator has no concerns with the proposed participation.

The submission typically includes information on the payment system the NBPSP intends to join, the proposed settlement model, the NBPSP's liquidity management arrangements and the operational resilience controls that support the participation in the payment system.

✓ **Completion of the regulatory assessment and obtaining a non-objection.**

The authority will review whether direct participation introduces additional risks that require supervisory mitigation. This assessment often focuses on three main areas: prudential requirements (safeguarding of

customer funds, wind-up plans), liquidity management (settlement exposure, prefunding arrangements) and operational resilience.

One common regulatory concern is the interaction between safeguarding requirements and settlement prefunding. NBPSPs typically safeguard customer funds in segregated accounts with commercial banks. When participating directly in a payment system, some of those funds may need to be placed in settlement accounts or prefunded positions to support payment processing. Authorities may therefore ask whether funds used for settlement remain properly safeguarded in the event of insolvency. In some jurisdictions, this question has required additional legal analysis because safeguarding frameworks were originally designed for indirect participation models where a sponsor bank handled settlement.

Another area of focus is liquidity management. Authorities often request evidence that the NBPSP can meet settlement obligations under stressed conditions. Operational resilience is also closely examined. Authorities will typically review how the NBPSP would respond to incidents such as loss of connectivity to the payment system, technology failures or fraud spikes.

NBPSPs frequently report that regulatory expectations can be difficult to interpret when direct participation by NBPSPs is new in a jurisdiction. Another common challenge is that regulatory review timelines are often unclear. If the authority does not provide indicative timelines or expectations, the review process may extend significantly beyond the PSO's onboarding schedule. This can jeopardise testing windows or certification slots that have already been allocated by the payment system.

💡 **PSO & authorities considerations for improvement**

Where possible, review timelines should be clearly communicated, with coordination among the regulator, central bank and PSO. Where deadlines exist or where time estimates are provided, the communication between the regulator and the NBPSP tends to be much more streamlined as both parties are working towards a defined timeline and have a sense of urgency.

3.3 Central bank approval

(Where a central bank account or settlement access is required, and where the central bank is not also the regulator)

The role of the central bank in the approval process varies depending on the payment system and the institutional setup in the jurisdiction. In some jurisdictions, the central bank supervises NBPSPs and operates the payment system. In others, the central bank operates the settlement infrastructure while a separate authority supervises NBPSPs. In these cases, a separate approval process with the central bank may be required.

Central banks may therefore assess the NBPSP in several capacities. They may act as the operator of the settlement system, the provider of settlement accounts and the payment system overseer. Each of these roles can introduce additional operational and technical requirements.

✓ **Approval of the settlement account application (if applicable).**

If a NBPSP seeks "full" direct access, including its own settlement account, obtaining approval for that account is a critical step in the onboarding process. The application typically requires detailed information on the NBPSP's liquidity management framework, operational procedures and settlement monitoring tools. The central bank

will review how the NBPSP plans to fund and defund its settlement account and how it will monitor its settlement position throughout the day.

The central bank and the NBPSP will also agree on the parameters governing settlement exposure. These parameters often include limits on net debit positions, prefunding requirements or collateral arrangements designed to ensure that the participant can meet its settlement obligations. The assumptions used to calculate liquidity buffers or collateral requirements may not always reflect the balance sheet structure of NBPSPs. This can require additional discussions to ensure that requirements are proportionate and compatible with the NBPSP's business model.

Because these discussions can involve several iterations between the central bank and the NBPSP, early engagement with the central bank is strongly recommended.

✓ **Confirmation of reporting obligations and obtaining testing certification.**

Settlement account access requires the NBPSP to provide intraday reporting as well as periodic reporting to the central bank or PSO. This may include liquidity positions, account reconciliation, transaction activity, operational incidents or compliance with settlement requirements. NBPSPs have to implement the necessary reporting processes and ensure that their internal systems can generate the required data in the correct format and frequency. In some jurisdictions, the infrastructure used to access the settlement account is operated by a separate technical service provider. This means that the NBPSP may need to integrate with additional systems in order to connect to the central bank infrastructure.

Before the account can be used in production, the central bank will typically require the NBPSP to complete testing procedures. These tests may include validating connectivity, confirming that settlement files can be transmitted correctly and verifying that the NBPSP can fund and defund the settlement account as expected. A common operational challenge arises because funding and defunding settlement accounts often involves manual processes. In some systems, participants have to send manual instructions or perform operational actions within defined time windows in order to move liquidity. This lack of automation can make both testing and daily operations more cumbersome. It can also increase operational risk, particularly during periods of high transaction volumes.

💡 **Central bank considerations for improvement**

Central banks can improve operational efficiency by modernising settlement account interfaces and enabling automated liquidity management processes. Providing clear documentation of funding procedures and testing requirements can also help NBPSPs prepare their systems more effectively before onboarding begins.

4. Technical set-up & testing checklist

4.1 Connectivity setup

Connectivity is the technical foundation of direct participation in a payment system. It enables a direct participant to securely exchange payment messages with a PSO or central bank. Connectivity is distinct from payment processing. Payment processing determines how transactions are created, validated and recorded in the participant's systems and the payment system itself. Connectivity determines how those messages are transmitted to the payment system, authenticated, encrypted and acknowledged.

Most payment systems have bespoke connectivity requirements. Many of these requirements were originally designed for banks and assume legacy infrastructure, static networks and on-premise deployments. Newer payment systems increasingly adopt modern communication models, including API-based interfaces (e.g. REST), which are easier to integrate at the application layer. However, it is important to distinguish between the interface used to exchange messages, the message format and the underlying network infrastructure over which those messages are transmitted.

In practice, a system may expose modern APIs while still relying on legacy connectivity infrastructure such as leased lines or proprietary network providers. In contrast, some systems may use older messaging protocols but operate over more flexible, cloud-compatible network setups. As a result, improving connectivity is not only about adopting modern APIs, but also about enabling more flexible, technology-neutral network and hosting options.

However, these more flexible, tech-neutral architectures are not yet the global norm. As a result, NBPSPs should address connectivity architecture early in the discovery phase. Connectivity design should not be treated as a purely technical implementation step late in the integration process. Architectural decisions made at this stage affect operational resilience, incident management, latency and long-term maintenance.

Connectivity typically involves several technical components that require both engineering design and operational planning.

✓	**Determination of network routing.**

Network routing determines the path payment messages take between the NBPSP and the payment system. Depending on the payment system, connectivity may rely on encrypted VPN tunnels, dedicated leased lines, Swift network connectivity, MPLS network connections, private cross-connects within data centres, cloud-based private connectivity (e.g. intra-cloud private endpoints or gateways) or payment system-mandated gateway devices. For example, some FPS require participants to connect through dedicated network providers that host routing infrastructure within specific data centres. In these cases, the NBPSP may need to establish a physical presence in the same data centre environment as the payment system infrastructure. In other cases, payment systems may support private cloud connectivity models, allowing participants to connect securely without requiring physical co-location. Where possible, PSOs should support both traditional and cloud-native connectivity options, provided they meet equivalent security and resilience requirements.

In some jurisdictions, regulatory or policy requirements require payments data and traffic to remain within national borders. This may require domestic data centre hosting or the installation of gateway appliances within the country. Although these requirements may serve policy objectives, they can significantly increase infrastructure complexity and cost for PSPs with international operations.

NBPSPs report that connectivity timelines are often delayed by factors such as long lead times for leased network lines, delays in data centre provisioning, hardware procurement, and installation of payment system-mandated routing devices. For example, the delivery and installation of physical gateway devices can take several months, particularly where supply chains are constrained. NBPSPs should therefore confirm connectivity routing requirements early in the discovery phase and include infrastructure procurement timelines in their implementation planning.

✓ **Definition of the IP configuration.**

IP configuration determines which network endpoints are authorised to communicate with the payment system. Many payment systems require participants to use static IP addresses that are pre-registered and allow-listed by the PSO. Only traffic originating from these addresses will be accepted.

This requirement can create challenges for cloud-native architectures, which often rely on dynamic scaling and rotating IP ranges. To address this constraint, NBPSPs commonly deploy network address translation (NAT) gateways or dedicated outbound proxy services that provide a fixed external IP footprint while allowing internal systems to scale dynamically.

Participants should also agree on failover IP addresses in advance. In some payment systems, changes to allow-listed IP addresses require manual approval by the PSO and may take several days. Without pre-approved backup IP ranges, this process can slow incident recovery during infrastructure failures.

✓ **Establishment of transport protocols and message exchange.**

Payment systems use a wide range of transport mechanisms for exchanging payment messages. These range from modern HTTPS-based APIs (REST or SOAP), secure file transfer (SFTP) for batch processing, message queue (MQ) infrastructure for asynchronous communication, to Swift FIN or ISO 20022 MX messaging over the Swift network, or even proprietary TCP-based protocols. Each transport model has different implications for system design. For example, MQ-based systems often require participants to maintain persistent connections and message queues, while file-based systems rely on scheduled file transfers and batch processing.

Some NBPSPs choose to use middleware or connectivity providers that abstract the payment system protocol behind an API layer. Others implement the payment system protocol directly in their internal systems. Direct protocol implementation may require several months of engineering effort but provides greater transparency and control over message processing. Gateway-based solutions may reduce implementation time but can introduce additional operational dependencies. From NBPSP experience, REST API-based connectivity models significantly reduce the technical barrier to entry and simplify future upgrades. They are easy to scale and well supported by modern software tools, while other connectivity methods (MQ, SFTP or proprietary network protocols) require more specialised infrastructure and integration effort.

✓ **Set up of security architecture and key management.**

Payment systems rely on cryptographic controls to ensure that payment messages are authentic and have not been modified in transit. Participants therefore use digital certificates to identify themselves and private cryptographic keys to sign payment messages. Because these private keys are highly sensitive, most payment systems require them to be stored in HSMs. An HSM is a specialised device that stores cryptographic keys

securely and performs cryptographic signing inside the device so that the private key never leaves the secure hardware.

While the number of payment systems that require physical HSM devices (as opposed to cloud-based alternatives) is decreasing, some still do. These devices often have to be configured through formal key ceremonies involving multiple parties and strict operational procedures.

NBPSPs frequently report that HSM deployment is one of the most complex parts of direct connectivity. Challenges include long procurement timelines for hardware devices, installation requirements within specific data centres, complex key ceremony procedures and manual certificate rotation processes. Because certificate lifecycles are often short, key rotation procedures must also be carefully planned before go-live.

💡 **PSO considerations for improvement**

Cloud-based solutions can reduce operational complexity, but there is an important distinction between cloud-hosted HSMs and key management services (KMS). Cloud HSMs are still HSM devices operated by the cloud provider and may retain similar complexity to on-premise deployments. In contrast, key management services (e.g. AWS KMS) abstract the underlying HSM infrastructure entirely and provide API-based key operations, while still meeting recognised security standards such as Federal Information Processing Standard 140-3 (FIPS 140-3), a widely recognised security standard for cryptographic modules, including the components used by HSMs and cloud key-management services to protect and use cryptographic keys. It defines four increasing levels of security assurance. PSOs should also clarify to which FIPS 140-3 level of assurance these solutions should be certified, with level 3 (stronger protection against physical tampering and unauthorised access to sensitive keys) providing an appropriate level of security, although the standard should be flexible over time. These services can significantly reduce procurement delays, operational overhead and costs for NBPSPs.

✓ **Optimisation of latency and performance.**

Connectivity architecture directly affects how quickly payment messages can be transmitted and processed. In many payment systems, participants must meet strict SLAs that define how quickly messages must be acknowledged or processed.

Latency can be introduced at several points in the connectivity chain. Each additional network hop, routing step or security operation increases the total time required to process a transaction.

For example, latency can increase when messages are routed through legacy network infrastructure, multiple gateway providers, geographically distant data centres, or HSMs performing message signing. These delays can become critical in FPS where payment systems impose tight response deadlines, whether for payment processing or overlay services. For example, the introduction of a one-second SLA for certain confirmation of payee services can become problematic and require an architectural redesign to reduce end-to-end latency. NBPSPs should design systems with sufficient performance headroom. A connection that meets current payment system SLAs during testing may struggle once transaction volumes increase or new overlay services are introduced.

NBPSPs therefore need to measure end-to-end processing time carefully during testing. This should include network latency, message processing time and cryptographic signing time within HSM devices. For example,

message signing operations inside an HSM may add several milliseconds to each transaction. When systems process thousands of transactions per second, these delays can accumulate.

Infrastructure placement also matters. If a payment system requires participants to connect through specific domestic data centres, the NBPSP should consider deploying infrastructure in the same geographic region to minimise network delays. Some NBPSPs operate dedicated connectivity nodes close to payment system infrastructure specifically to optimise latency.

> 💡 **PSO considerations for improvement**
> PSOs can support better performance by making clear latency expectations and testing methodologies available for participants. Providing realistic performance benchmarks and load-testing environments allows participants to verify that their systems can meet payment system requirements before going live. Where possible, payment systems should also minimise unnecessary network routing steps and avoid infrastructure requirements that introduce avoidable latency without improving resilience or security.

Across jurisdictions, NBPSPs report recurring challenges when establishing connectivity with payment systems. Payment system documentation may assume the use of on-premise data centres, static server configurations or proprietary network appliances.

Participants also encounter requirements that add complexity without necessarily improving security or resilience. These can include mandatory physical gateway devices, domestic routing appliances, rigid static IP address policies or authentication mechanisms designed around legacy infrastructure. In some cases, payment systems assume specific operating environments such as Windows-based servers or long-lived stateful processes, which may not align with modern microservice-based architectures commonly used by NBPSPs.

The most time-consuming aspect of connectivity is often not building the transport layer itself, but understanding and interpreting payment system and PSO expectations. NBPSPs spend significant effort on clarifying operational expectations and reconciling modern cloud architectures with infrastructure assumptions embedded in legacy payment systems. Early, transparent engagement with PSOs and regulators on architectural design choices can significantly reduce friction later in the process.

> 💡 **PSO & regulatory considerations for improvement**
> PSOs and regulators can reduce these challenges by adopting technology-neutral connectivity requirements and security standards that focus on outcomes rather than prescribing specific infrastructure. For example, payment systems can require recognised cryptographic standards such as FIPS-certified key management without mandating specific hardware devices or data centre environments. Operational resilience, system uptime, disaster recovery and business continuity requirements should similarly be agnostic to whether a participant connects using physical infrastructure or cloud-based environments, provided the participant can demonstrate equivalent security and resilience controls.

4.2 Functional setup

While connectivity defines how messages travel between systems, the functional setup determines how a participant behaves within the payment system. At this stage, a NBPSP should look at translating payment system rules into executable system logic. The direct integration has to work predictably across thousands of scenarios, not only the successful “happy path”. It also needs to provide operational teams with the tools and controls to detect, investigate and resolve issues at scale. Across markets, NBPSPs report that the biggest delays at this stage are caused by unclear payment system documentation, late discovery of rulebook obligations, and

underestimation of the effort required to support operational flows such as returns, recalls, trace requests and reconciliation.

✓	**Implementation of message mapping and validation.**

A NBPSP needs to be able to translate its internal payment data into the message format required by the payment system and validate that outgoing messages comply with payment system specifications. This applies whether the payment system uses ISO 20022, Swift MT messages, or a proprietary domestic format.

International NBPSPs report three common challenges during message mapping. First, even when payment systems use ISO 20022 messaging standards, they often introduce local variations or additional validation rules. These differences may not be obvious from generic ISO 20022 documentation. Participants only discover these once they start failing certification test cases.

Second, payment system documentation often assumes familiarity with legacy message types. This leads to "reading between the lines". Engineers may therefore need several rounds of clarification to understand how specific message fields should be populated.

Third, for international NBPSPs, domestic rails may not support all the data elements needed for sanctions screening, AML checks, or dispute handling. This usually means that NBPSPs offering international payments have to spend significant time mapping their internal payment data to the message formats expected by the payment system. Many domestic payment systems implicitly assume that participants originate payments using traditional banking formats such as CBPR+ ISO 20022 credit transfer files. In practice, NBPSPs often operate API-based payment platforms or internal data models that differ significantly from these formats. As a result, NBPSPs may need to build additional translation layers that convert their internal payment instructions into the payment system's expected message structure. For example, a cross-border payment initiated through a NBPSP's API may contain structured beneficiary information, FX data or compliance metadata that does not directly map to the fields available in a domestic payment message. Engineering teams therefore need to design message transformation logic that preserves the required compliance and reconciliation information while still complying with payment system validation rules.

💡 **PSO considerations for improvement**

PSOs can significantly reduce integration friction by going beyond static documentation and providing comprehensive test suites covering multiple scenarios (including error cases and edge conditions), along with expected input and output messages. While static example messages are helpful, they typically represent only a single use case and do not capture the full range of variations encountered in practice. Machine-readable validation rules or contract testing tools enable participants to automatically verify compliance.

Where domestic message formats cannot support certain data elements, payment system rules should define which information is mandatory and what compensating controls are acceptable. This is particularly important for cross-border payments subject to the Financial Action Task Force's Recommendation 16 on payment transparency, which requires specified originator and beneficiary information to accompany payments through the payment chain. Payment system rules and technical specifications are important enablers for participants to meet applicable Recommendation 16 requirements and should identify any permitted alternative or compensating controls where the domestic message format cannot carry all required information.

✓ **Design and automation of unhappy path handling.**

Unhappy paths are a part of payment system operations. These include returns, recalls, reversals, trace requests, inquiries ("where is my money?"), and fraud-related or otherwise suspicious messages. Functional maturity is defined far more by how these flows are handled than by whether a participant can send a successful payment.

Common challenges experienced by NBPSPs are that payment systems differ dramatically in how structured unhappy paths are. Some payment systems define structured message flows for returns, reversals and trace requests. These flows are formally documented and included in certification testing. This approach allows participants to automate exception handling and reduces ambiguity. Other payment systems rely on manual processes. For example, participants may need to exchange emails or call other participants to investigate missing payments or initiate reversals. This approach introduces operational overhead and does not scale well as transaction volumes grow. In some markets, it is so pronounced that operational teams can become overloaded by daily manual inquiries where payment systems don't provide codified inquiry messaging.

Another recurring issue is that payment system documentation typically describes successful payment paths clearly, but is weaker on failure sequencing, retries, duplicates, and the precise meaning of acknowledgements. As a result, NBPSPs sometimes discover important behaviours, such as duplicate message handling or retry logic, during certification testing or even after go-live. This can delay the whole integration and is particularly problematic when there is a defined timeframe by which a participant needs to go live after application.

💡 **PSO considerations for improvement**

PSOs can significantly improve operational efficiency by codifying unhappy path scenarios as formal message flows wherever possible. Certification processes should test these scenarios explicitly. Where payment systems standardise returns, inquiries and non-payment messages, this enables participants to automate issue handling and reduce operational risk. Where manual processes remain necessary, payment systems can still reduce friction by standardising templates, timelines and escalation routes, and by publishing clear definitions of what constitutes a return, a reversal, a recall and a trace in that specific system.

✓ **Implementation of liquidity and settlement logic.**

Any participant has to correctly process settlement reports, monitor prefunding or collateral requirements where applicable, and manage net positions in deferred settlement systems. Therefore, the functional setup has to reflect the settlement mechanics of the payment system. These mechanics determine the financial exposure that the NBPSP must manage.

One of the issues NBPSPs face is that operational realities are not visible from technical documentation, but only get exposed during implementation and testing stages. In some systems, settlement funding and defunding is still manual and time-bound. Even in mature markets where NBPSPs are provided with their own settlement account, funding and defunding that account can require frequent manual balance checks and operational actions during the day. In other cases, limited funding windows can create a real risk of running out of settlement liquidity for customer payouts, especially when volumes spike unexpectedly. In payment systems with real-time gross settlement, this risk is entirely mitigated. In contrast, in deferred net settlement systems, the key challenge is timing risk: outflows may be executed while inflows are delayed, leaving the participant to cover the gap. This can become acute during payment system incidents or when inbound messages are delayed due to connectivity issues.

To manage these risks, NBPSPs typically implement automated settlement position dashboards, alert thresholds, and clear escalation triggers that connect operational teams, treasury teams and engineering. NBPSPs should model worst-case liquidity days and payment system incident scenarios and aim to document funding playbooks in the form supervisors and central banks expect, because in some jurisdictions written operational manuals are necessary in order to obtain approval.

💡 **PSO & central bank considerations for improvement**

To help NBPSPs and other participants meet their liquidity and settlement obligations, PSOs and central banks could provide better automation and real-time tools for liquidity visibility. Several NBPSPs report that conservative buffer requirements are often driven by poor visibility rather than intrinsic risk, which leads to NBPSPs having to hold excessively large liquidity buffers to account for system error margins. Where payment systems support near real-time position reporting and clear intraday funding processes, participants can run leaner and safer liquidity models. Central banks can also reduce operational risk by modernising settlement account funding interfaces and by clarifying funding windows and cut-offs transparently.

✓ **Establishment of automated reconciliation.**

Reconciliation is the control layer that ensures the NBPSP's internal records match payment system records. Clearing and settlement are separate processes, and mismatches can occur even when connectivity appears healthy. Participants must therefore verify that all transactions reported by the payment system are reflected correctly in their internal ledgers.

NBPSPs frequently encounter challenges because payment system reporting is not always designed with participants in mind. Reports may be fragmented across multiple files, portals or endpoints, and definitions may not align directly with internal product data. For example, the payment system may report a successful transaction, but the participant's internal system may not have processed the corresponding acknowledgement message correctly. This creates an ambiguous state that requires investigation. Reconciliation logic must therefore handle scenarios such as duplicate messages, delayed acknowledgements, partial failures and late reversals. Where payment systems lack permanent test environments, reconciliation edge cases may only appear in production.

💡 **PSO & central bank considerations for improvement**

NBPSPs have reported a much more seamless integration where payment systems build in automation that provides full transparency on exactly why a payment failed (e.g. destination account does not exist), rather than forcing NBPSPs to rely on manual email-based inquiries. In addition, standardised reporting formats and "reconciliation starter packs" (sample files, mapping guides, common mismatch scenarios), can significantly reduce the operational risk for new entrants.

✓ **Ensuring adequate load handling and capacity management.**

Direct participation requires a system that can handle not only normal transaction volumes, but also peak periods, unexpected spikes and payment system-level stress events. Load handling is therefore central to maintaining payment system stability and meeting performance obligations.

A common challenge for NBPSPs is that payment volumes are rarely evenly distributed, as many NBPSPs are newer, grow and expand more quickly or address a less predictable part of the market, which can lead to unexpected behaviour or spikes in volumes.

In an FPS, these spikes have to be absorbed in real time. In deferred settlement systems, volume spikes can create liquidity pressure in addition to processing load. Payment system incidents can also create load surges. For example, if a payment system experiences a temporary delay and later recovers, queued messages may be released simultaneously, creating a sudden spike in processing demand.

NBPSPs should therefore design systems to scale horizontally where possible, and to measure performance under realistic stress conditions. Load testing should not only simulate average volumes but also extreme but plausible peak scenarios. Participants should monitor queue lengths, processing times and rejection rates in real time, and define internal thresholds that trigger investigation before payment system-level SLAs are reached.

💡 **PSO considerations for improvement**

Payment systems can support participants by offering realistic performance testing environments and publishing typical peak patterns. When payment systems impose penalties for excessive timeouts or rejects, transparent documentation of how these metrics are measured, helps participants calibrate their systems appropriately and can avoid any risk to the participant or to the system.

4.3 Testing and certification

Most payment systems require formal certification before go-live. This typically includes message validation, scenario testing and submission of test evidence to the PSO. However, NBPSP experience shows that certification testing alone is rarely sufficient. Certification environments usually validate whether the participant's integration complies with the payment system specification, but they do not fully replicate real-world operating conditions. Participants therefore need to conduct additional internal testing beyond the minimum required by the payment system.

There are two main challenges for testing. First, test environments are often scarce. Payment systems may have limited slots available for testing, which means that a NBPSP either has to rush through its preparation to meet a testing slot or remain idle for months after their preparation work is finished.

Second, there is often a forced dependency on banks to perform pre-production testing. Some payment systems require "buddy testing" with a large incumbent bank, which can take two to three months to schedule. To reduce these delays, PSOs could provide a dummy participant, "test bank", or emulator interface. This allows NBPSPs to simulate and validate payments against payment system rules on-demand, without depending on other participants.

✓	**Completed functional certification testing.**

Before go-live, NBPSPs have to demonstrate that all supported message types and flows behave correctly. This includes both outgoing and incoming messages. In practice, this means executing dozens - if not hundreds - of predefined test cases. In some markets, engineers have reported running between 300 and 1,000 test scenarios for relatively simple integrations. These cover not only successful payments, but also returns, recalls, rejections, format errors and timeout scenarios.

A common challenge is that payment system documentations do not always fully describe edge cases. NBPSPs sometimes discover inconsistencies during certification, particularly in unhappy path flows. Where no permanent test environment exists - as is often the case when PSOs only provide time-limited test slots - participants have to rely heavily on internal simulators. This usually has its limits because real-world behaviour may differ in production. Therefore, PSOs and central banks should be encouraged to maintain a permanent test environment.

NBPSPs should also build internal test simulators that mimic payment system behaviour as closely as possible. Participants should not rely solely on payment system test windows. They should document test evidence carefully, because most payment systems require formal submission and sign-off before giving the green light.

✓ **Conducting realistic load and performance testing.**

In addition to functional certification, NBPSPs must ensure that their systems can operate reliably under realistic transaction volumes. Testing should simulate both normal operating conditions and stress scenarios. For example, NBPSPs should test how their systems behave when payment volumes are two or three times higher than on an average day. They should simulate scenarios where the payment system itself experiences a delay and then releases a backlog of messages all at once.

Load testing should also examine how queues behave under stress. For example, if an upstream service slows down for 10 to 15 minutes, does the integration recover smoothly once the service is restored? Or does the system create growing backlogs and timeouts that lead to SLA breaches? These scenarios are common during incidents and should be rehearsed.

💡 **PSO & central bank considerations for improvement**

PSOs and central banks can help by providing clarity on how performance metrics are measured and what constitutes a breach. When participants understand precisely how latency and rejection thresholds are calculated, they can calibrate internal monitoring more effectively.

✓ **Test failure scenarios and disaster recovery.**

NBPSPs should simulate component failures and observe how the system reacts. For example, if the database becomes temporarily unavailable, does the integration stop safely and resume processing without creating duplicates? If a confirmation message is delayed, does the system avoid crediting funds prematurely? If a network route fails, does traffic switch to a secondary path as designed? If a primary region becomes unavailable, does the failover connectivity, certificates and routing configurations work correctly in the backup environment?

NBPSPs report that many early production incidents occur not because of message formatting errors, but because certain infrastructure assumptions were never tested under failure conditions. This exercise should be as comprehensive as possible.

💡 **PSO & regulatory considerations for improvement**

PSOs and regulators can support resilience by encouraging regular disaster recovery exercises that are proportionate and practical. In many jurisdictions, formal disaster recovery testing is required only once a year and often involves extensive documentation, advance notice and submitting of supporting evidence. While this ensures planning security, it can also make testing infrequent and compliance-driven rather than

operationally useful. A more effective approach is to conduct smaller, scenario-based tests more regularly, such as simulating loss of a primary data centre, network routing failure or HSM unavailability. These exercises build operational “muscle memory” and expose weaknesses earlier, rather than concentrating all testing effort into a single annual event. Smaller exercises in combination with a permanently available, high-quality testing environment would contribute to the resilience of the payment system and its participants.

5. Go-live

✓	**Gradual and controlled rollout through penny testing.**

Even comprehensive testing cannot perfectly replicate production conditions. For this reason, go-live should be gradual and controlled. NBPSPs should begin with low-value “penny tests” to confirm real settlement behaviour. These are real transactions processed end-to-end in production, but with minimal financial exposure. The purpose is to confirm that payment messages are transmitted, acknowledged and settled as expected, and that internal ledger entries match payment system reports.

In practice, some behaviours only become visible in production. For example, NBPSPs have observed timing differences in messaging acknowledgements, unexpected sequencing of confirmation messages, or minor variations in settlement reporting that were not visible in test environments. Penny testing allows these issues to surface before high-value transactions are processed. Once penny tests are successful, volumes should be increased gradually.

Unexpected behaviour often appears only once real counterparties and real timing conditions are involved. In some payment systems, test environments simulate only a limited number of participants. When the system goes live, messages must be exchanged with many other banks and payment service providers whose systems may behave differently from test simulators.

However, technical go-live does not automatically equal commercial readiness. A key challenge for NBPSPs is incumbent participants failing to update their routing table, participant directories or customer-facing user interfaces to recognise the new NBPSP. As a result, customers of other participants may initially be unable to send payments to accounts hosted by the new participant.

💡 **PSO considerations for improvement**

PSOs can coordinate ecosystem readiness before go-live. Participant directories, routing tables and payment system reference data should be updated centrally and distributed to all participants regularly. This helps ensure that new entrants can begin operating on equal terms with existing participants from the first day of production.

6. Post-launch

6.1 Maintenance and ongoing compliance

Direct access is not a one-time project. Once a NBPSP becomes a direct participant, it enters into an ongoing operational and regulatory commitment. Payment systems evolve continuously as they introduce new services, technical upgrades and regulatory requirements. Participants are expected to adapt their internal systems accordingly. As a result, maintaining a direct connection requires ongoing engineering, operational and compliance resources. NBPSPs have reported that the long-term maintenance burden can be higher than initially expected. Integration work does not end at go-live. This should be taken into account for the initial business case.

New payment system features, message format changes and operational requirements continue to require development work. The cost of maintaining a direct connection can therefore increase over time as payment systems introduce additional features and reporting requirements. However, as transaction volumes grow, the economies of scale associated with direct participation generally improve.

✓ **Management of system and mandatory updates.**

Payment systems regularly introduce technical and operational updates. These can include changes to message formats, new overlay services (e.g. confirmation/verification of payee, request to pay), SLA adjustments (e.g. reducing response times), fraud reporting enhancements or regulatory reporting. These updates are often mandatory and subject to fixed implementation deadlines.

NBPSPs should therefore monitor payment system change announcements closely and allocate engineering capacity for implementation. Failing to meet upgrade deadlines can lead to operational restrictions or suspension from the payment system. However, some NBPSPs have reported missing payment system change announcements because PSOs and central banks only communicated the changes via the local banking associations, which do not always allow NBPSPs to become members. Therefore, PSOs should ensure that any payment system changes or upgrades are communicated to *all* participants and avoid going only via industry groups that do not represent the whole ecosystem.

💡 **PSO considerations for improvement**

PSOs and regulators can reduce implementation risk by publishing clear release cycles and providing early draft specifications, which allow participants to prepare gradually. Where possible, providing machine-readable specifications, example messages and regression test cases reduces interpretation risk. This is particularly helpful for NBPSPs who often do not have the same level of bank-specific (infrastructure) knowledge and therefore need help “reading between the lines”. Ultimately, all participants benefit when updated documentation explains not only what changed, but why and where in the message flow the impact occurs.

✓ **Maintaining certificate and key lifecycle processes.**

Certificates and cryptographic keys used for connectivity and message signing have to be renewed periodically. These certificates are used to authenticate participants and sign payment messages. In systems that rely on HSMs, renewal may involve formal key ceremonies and coordination with PSOs. Errors during certificate

replacement can disrupt connectivity and temporarily disconnect the participant from the payment system. For example, if a certificate expires before the new one is correctly installed, the payment system may reject all incoming and outgoing messages until the issue is resolved. NBPSPs often find that certificate renewal is one of the highest operational risks because it is infrequent and manual, whereas NBPSPs look for automation to the greatest extent possible.

💡 **PSO & central bank considerations for improvement**

PSOs and central banks can reduce friction by allowing certified cloud-based key storage solutions and by standardising renewal processes. Clear guidance on renewal timelines and overlap handling reduces outage risk for NBPSPs.

✓ **Recurring disaster recovery and resilience testing.**

Resilience testing should not end at go-live. Systems change over time, and infrastructure evolves. Participants should periodically test failover scenarios, database recovery procedures, routing redundancy and HSM resilience. In practice, NBPSPs benefit from breaking down large disaster recovery tests into smaller, recurring exercises. For example, a quarterly simulation of one component failure builds operational readiness much more effectively than an annual full-system test. Many regulators currently require formal disaster recovery testing only once per year. Although this provides an important level of oversight, it can lead to exercises that focus heavily on documentation rather than operational effectiveness.

💡 **PSO and central bank considerations for improvement**

PSOs and central banks can strengthen resilience by encouraging routine, proportionate testing. Allowing structured, recurring partial tests helps participants maintain readiness without excessive administrative overhead. In addition, providing a permanent testing environment, would allow NBPSPs to experiment with enhancements to their direct integration without introducing risk to the payment system or its participants.

✓ **Maintaining liquidity and financial controls.**

Post-launch liquidity management requires continuous monitoring. Transaction volumes can grow rapidly once direct access is enabled, because the impact of a direct integration on customers can be transformative. New use cases or market expansions can also change the balance between inbound and outbound flows.

NBPSPs should regularly review liquidity stress assumptions and update models as volumes evolve. Monitoring dashboards, alert thresholds and escalation procedures should be updated as volumes evolve.

💡 **PSO and central bank considerations for improvement**

By providing timely information, central banks, as settlement account providers, and PSOs enable NBPSPs to monitor their liquidity position throughout the operating day. The information should cover settlement and prefunding account balances, outstanding settlement obligations and - where applicable - remaining headroom against payment system limits. It is helpful if information is available through machine-readable interfaces that participants can integrate into their own treasury systems.

✓ **Ongoing compliance and reporting obligations.**

Direct participants are often required to submit periodic security attestations, complete annual or biennial penetration tests, provide incident reports and execute mandatory recertification testing. NBPSPs report that these processes can be highly manual and documentation-heavy. Reporting formats also tend to be bespoke to every payment system. While most PSOs require similar attestation, testing or reporting, the slight differences across jurisdictions make a globally uniform approach impossible for firms operating in multiple jurisdictions. This means these annual compliance cycles may require weeks of preparation to meet obligations in various jurisdictions.

💡 **PSO and regulatory considerations for improvement**

Supporting the automation of recurring compliance tests can improve their quality while reducing costs for PSOs and regulators. Machine-readable validation frameworks and repeatable certification scripts are preferable to one-off manual evidence reviews. They also verify compliance much better than a manual evidence check.

✓ **Contribution to operational and governance processes.**

Direct participants are typically expected to contribute to payment system governance processes. These may include technical working groups, rulebook committees, fraud forums and change advisory boards. Active NBPSP participation helps ensure that new payment system features and rule changes reflect the needs of all participants, not just incumbents. It means that NBPSPs can proactively influence upgrades and enhancements to the payment system in a way that does not just work for incumbents, but also for newer players. It also means that they are informed of upcoming changes much earlier, which can help them meet their obligations ahead of the deadline.

However, governance participation can create a significant resource burden, particularly for smaller NBPSPs. Many meetings require preparation, technical review and follow-up implementation work. NBPSPs should allocate dedicated ownership for payment system participation and ensure knowledge is documented internally rather than concentrated in individuals.

💡 **PSO considerations for improvement**

PSOs should ensure that governance processes are transparent and proportionate, and that non-bank participants can contribute meaningfully rather than have a symbolic representation only. Ensuring balanced representation helps payment systems evolve in a way that supports innovation while maintaining system stability.

Conclusion

Expanded access to payment systems for NBPSPs is slowly becoming increasingly common. Across jurisdictions, experience shows that well-designed access frameworks can deliver meaningful improvements in competition, efficiency, resilience and financial inclusion, while supporting the broader objectives of the G20 Roadmap for Enhancing Cross-Border Payments.

While implementation of enhanced access frameworks is not without complexity, this report highlights a fairly consistent path to including NBPSPs among key payment systems' direct participant base. Authorities need to balance the benefits of broader participation with maintaining the integrity and resilience of their payment systems. That balance is best achieved through proportionate, risk-based approaches that apply consistent requirements across participants, regardless of institutional form.

The insights from jurisdictions that have already enabled direct access for NBPSPs or have taken steps in this direction are useful. Successful models have not lowered standards, but have adapted them. They have modernised technical requirements and introduced more transparent and predictable application and onboarding processes. They allowed regulated NBPSPs to join the payment system provided they met the same technical, financial, operational and risk management requirements as their bank counterparts. The best practices in Part 1, highlighted by jurisdictions that have enabled or are in the process of enabling direct access for NBPSPs, also provide insights into the impact of granting settlement account access to NBPSPs.

Crucially, some jurisdictions highlighted that NBPSPs have not introduced additional risk to their payment system, provided they put the right safeguards and regulatory oversight in place. In addition, some jurisdictions confirm that it is the maturity of the applicant and completeness of information provided that will dictate whether an application for direct access is successful, not whether an applicant is a bank or NBPSP.

Part 2 covers a detailed overview of the process of obtaining direct access as a NBPSP, informed by real-world experiences from NBPSPs who successfully went through the process. While much of the global policy discussion has focused on ***whether*** access should be expanded, assessing the benefits, risks and barriers of expanding access, the practical experience of NBPSPs demonstrates that ***how*** access is granted is equally important. One NBPSP case study shows that building a direct connection is a labour-intensive and costly process, averaging between $1-1.3 million per connection. However, the resulting decrease in per transaction costs (between 40-60%) and increase in speed have a considerable impact on end-users.

The checklist for NBPSPs highlights the challenges NBPSPs have faced in each step of the six-part journey of obtaining direct access, and how central banks, regulators and PSOs can help reduce unnecessary obstacles and complexity. The most recurring friction points are unclear or bank-centric documentation, fragmented application processes, limited testing environments, conservative liquidity requirements and misalignment between regulatory and payment system expectations. By making these challenges explicit, the toolkit provides a basis for both NBPSPs and authorities to address them proactively.

A key insight from this report is that expanding access is a two-sided process. Policy reform alone is not sufficient if onboarding remains operationally complex, opaque or inefficient, or if the legal treatment of safeguarded funds is left ambiguous. Equally, NBPSPs have to be adequately prepared to meet the responsibilities - operational and financial - that come with direct participation. The most effective frameworks are therefore those that align policy design with operational implementation, reducing unnecessary friction while maintaining robust safeguards.

Looking ahead, continued progress will depend on a few key areas. Firstly, regulatory and supervisory frameworks need to continue evolving to recognise the growing role NBPSPs play in the ecosystem. Clear, proportionate and well-coordinated regulatory requirements and supervision enables central banks, regulators and PSOs to rely on existing oversight rather than duplicating it.

Secondly, modernising infrastructure and access models will be critical. Tech-neutral requirements, connectivity compatible with cloud setups, and improved liquidity and reporting tools can significantly lower barriers to entry. Setting clear outcomes, rather than prescribing (outdated) tools, is key to maintaining resilience and security.

Thirdly, international cooperation can spur the next wave of enhanced participation. As payment systems evolve and interlink, aligning access frameworks and reducing fragmentation will be important. Developments such as Europe's *Memorandum of Understanding (MoU) on information sharing between national supervisory authorities and national central banks to support NBPSPs access to central bank operated payment systems*[13] are a step in that direction. More international collaboration could reduce the duplication of information NBPSPs have to share with authorities and PSOs to obtain access to payment systems, accelerating increased competition and reduced concentration risk.

Lastly, while access to payment systems where NBPSPs can settle and clear on their own behalf is an important step, there is still continued reliance on bank partners: in most jurisdictions, NBPSPs still have to safeguard their customers' funds with a commercial bank. A few countries allow - and some even oblige - NBPSPs to hold those funds with central banks. However, this goes beyond the current scope and mandate of the PIE task force.

[13] European Banking Authority (2025) - *MoU on information sharing in support of non-bank payment service providers access to central bank-operated payment systems*

References

Australian Treasury (2023), *Payments System Modernisation: Regulation of payment service providers*.

Australian Treasury (2026), *Payments licensing reforms*.

Banco Central do Brasil (2023), *Manual de Redes do Sistema Financeiro Nacional*.

Banco de México (2017), *Regulation 14/2017 - Rules of the interbank electronic payment system (SPEI)*.

Bangko Sentral ng Pilipinas (BSP), *National Retail Payment System framework*.

Bangko Sentral ng Pilipinas (BSP) (2021), *No One Left Behind: Digital Payments Transformation*.

Bank Indonesia (2021), *Regulation concerning the implementation of Bank Indonesia -FAST Payment*.

Bank Indonesia (2021), *Regulation concerning Payment Service Providers*.

Bank Indonesia (2025), *Regulation concerning the regulation of the payment system industry*.

Bank Indonesia (2026), *Regulation concerning the implementation of Bank Indonesia-FAST Payment*.

Bank of Canada (2021), *Retail Payment Activities Act (RPAA)*.

Bank of England (2021), *Bank of England Settlement Accounts*.

Bank of England (2024), Reviewing access to RTGS accounts for settlement.

Bank of England (2025), *Access policy for RTGS settlement accounts and services*.

Bank of England (2025), *Access to UK payment systems for non-bank payment service providers*.

Bank of England (2025), *Response to the discussion paper on reviewing access to RTGS accounts for settlement*.

Bank of England (2025), *Real-Time Gross Settlement (RTGS) system and CHAPS Annual Report 2024/25*.

Bank of Japan (2024), *Payment and Settlement Systems Report*.

Bank for International Settlements (2025), *Enhancing cross-border payments: state of play and way forward*.

Bank for International Settlements (2026), *Enhancing cross-border payments step by step: insights from the 2025 monitoring survey*.

Committee on Payments and Market Infrastructures (CPMI) (2022), *Improving access to payment systems for cross-border payments: best practices for self-assessments*.

Committee on Payments and Market Infrastructures (CPMI) (2025), *Brief No 10: Moving on up: results of the 2024 cross-border payments monitoring survey*.

Committee on Payments and Market Infrastructures (CPMI) / PIE Taskforce (2026), *Expanding access to payment systems: considerations for a path forward*.

EBA Clearing, *RT1*.

European Banking Authority (2025), *Memorandum of Understanding on the cooperation framework for information sharing between national supervisory authorities and national central banks in support of the access of non-bank payment service providers to central bank operated payment systems*.

European Commission (2020), *EU Retail Payments Strategy*.

European Central Bank (2024), *Policy on access to central bank-operated payment systems by non-bank PSPs*.

European Union (2024), *Instant Payments Regulation (EU) 2024/886*.

Financial Stability Board (2024), *Recommendations for regulating and supervising bank and non-bank PSPs offering cross-border payment services*.

Payments Canada (2022), *Expanded access to critical payment infrastructure will drive competition and growth in Canada*.

Government of Canada (2022), *Expanding membership eligibility in Payments Canada*.

Monetary Authority of Singapore (2019), *Payment Services Act*.

Monetary Authority of Singapore (MAS) (2020), *Non-bank financial institutions to have access to FAST and PayNow*.

Reserve Bank of Australia (2019), *NPP Functionality and Access Consultation: Conclusions Paper*.

Reserve Bank of Australia (2024), *Payments System Board Annual Report – 2024*.

World Bank, *Project FASTT: Case Studies*.

Zengin-Net (2022), *Expansion of access to fund transfer service providers*.

Zengin-Net (2023), *PFMI disclosure report*.