

Insight report

Assured Science:
The Network Behind Always-On Finance

From transaction-critical performance to resilient, secure and intelligent connectivity

What financial-services discussions and independent industry evidence reveal about the networks supporting real-time transactions, distributed operations and emerging data workloads.

Explore the report

Evidence and methodology

This report examines the connectivity challenges facing financial institutions with distributed operations, cross-border service dependencies and increasingly hybrid technology estates. It focuses on enterprise and inter-site connectivity, application performance, resilience, secure access and coordination across network providers. Specialist exchange-colocation infrastructure and the core systems of payment networks have different requirements and sit outside the scope of managed enterprise connectivity.

Our research used AI-assisted audience profiling and inferential analysis to classify 25,675 publicly expressed online opinions relating to senior technology, infrastructure and network leaders in financial services. The analysis covered X, Quora, Reddit, Bluesky, TikTok and Threads over the twelve months ending 12 October 2026. These are modeled interpretations of public discussion, not direct survey responses, verified professional identities or audited evidence of what institutions have deployed. Their statistical representativeness has not been independently established.

The opinion analysis provides directional themes for a wider international audience; it is not presented as a global sample. We test the commercial and technical implications against independent international research and guidance from BIS/CPMI, the Basel Committee on Banking Supervision (BCBS), the Financial Stability Board (FSB) and other relevant authorities. Regional rules and examples are identified as such. Findings from different sources are not directly comparable or evidence of causal relationships.





Executive summary

Financial services across markets are becoming more immediate, continuous and interconnected. Fast payments, hybrid applications, distributed branches and data-intensive services increase the need for networks that perform predictably and remain manageable when something fails. Connectivity needs to be understood through the transaction, financial service or customer journey it supports, not simply whether a circuit is available.

Our modeled opinion analysis identifies real-time payments and AI-related workloads as prominent network planning themes. Separately, BIS/CPMI analysis of international payment statistics shows fast payments gaining ground, particularly in emerging-market and developing economies. The two sources measure different things, but together frame a practical question for financial institutions: can they demonstrate the performance, resilience and oversight of the networks supporting critical services?

Five connected priorities emerge from the research, highlighting the capabilities financial institutions need to sustain secure, responsive and resilient digital services:

1. **Define performance around critical financial services.** Translate payment, customer and application requirements into explicit network service objectives.
2. **Make resilience demonstrable.** Map dependencies, test recovery and relate incidents to business impact rather than relying on uptime measures alone.
3. **Coordinate hybrid and multi-provider operations.** Establish consistent ownership and visibility across branches, cloud platforms, carriers and external partners.
4. **Build security and governance into connectivity decisions.** Apply appropriate access controls, third-party accountability and forward-looking cryptographic planning.
5. **Prepare the network for AI and data-intensive workloads.** Improve telemetry, skills and operational safeguards before expanding automation.

Taken together, the findings suggest that always-on finance requires an operating model capable of demonstrating what the network delivers, diagnosing where service quality declines and restoring critical functions through clear accountability. No single access technology or security product can provide that assurance on its own.



Why this matters

For a financial institution, degraded connectivity can affect far more than employee productivity. It may interrupt access to customer accounts, delay a payment-related workflow, reduce the timeliness of fraud signals or complicate recovery during an incident. Different workloads have different tolerances for delay and disruption, so generic performance targets are a poor substitute for service-specific requirements.

The strategic opportunity is to connect application priorities, network and cloud operations, security, third-party relationships and recovery planning within one evidence-led operating model. Global institutions need confidence that important services can be sustained across locations, suppliers and changing demand without assuming that every application requires identical technical characteristics.

The objective is to make network performance measurable and accountable as part of financial service delivery, supporting innovation and customer confidence while reducing avoidable operational complexity.

Expereo perspective:

“

Financial institutions have to maintain continuous customer services alongside scheduled processing and system maintenance. The challenge is proving that essential services remain usable when something fails. A network availability figure cannot show whether customers can complete a payment or access their accounts. That requires evidence across the full service, including shared dependencies, backup capacity and the time needed to restore normal operation.

”

Julian Skeels
Chief Digital Officer,
Expereo



Theme 1:
The rise of always-on financial services

Real-time services make connectivity expectations more demanding, but the right design starts with the workload.

Financial services increasingly operate beyond traditional working hours and span mobile channels, branches, partners and cloud-hosted applications. Outcomes depend on more than transaction-processing platforms alone: identity services, customer-data access, fraud systems, network reachability and third-party integrations can all shape what customers experience.

Network leaders should therefore identify which services are genuinely time-critical, and precisely how they depend on connectivity. Instant payments, retail account access, customer support, reporting and specialist trading have different traffic profiles and consequences when performance declines. A sound strategy makes those differences explicit rather than imposing a universal latency or availability target.

Real-time payment demands are becoming more prominent

In our US-based opinion analysis, 55% of classifications anticipated a moderate increase in connectivity performance demands from real-time payments, and 45% a significant increase. These categories represent inferred expectations, not directly measured bandwidth growth, transaction throughput or latency.

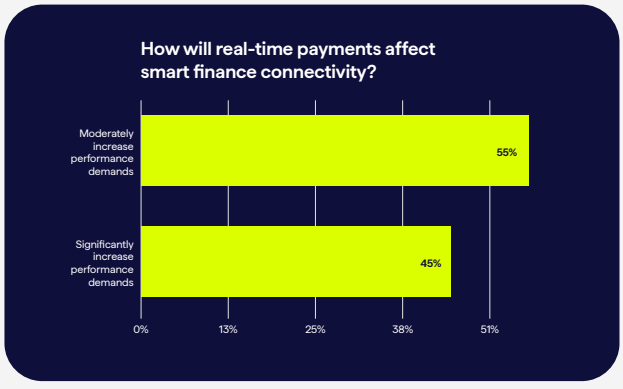


Figure 1. Expected impact of real-time payments on connectivity demand (55% moderate; 45% significant).

International context supports taking this challenge seriously. BIS/CPMI analysis of payments statistics shows that fast payments continue to expand, while its work on linking fast payment systems across borders highlights the importance of governance and operational coordination. These developments create demands for dependable access to payment services and associated data, although the specific network requirements depend on the role an institution plays in the payment chain.

Real-time processing does not imply that every service requires the same network profile. A payment initiation channel, an anti-fraud feed and a clearing connection may have different performance, resilience and recovery needs. Their dependencies also extend beyond WAN links to identity platforms, application gateways, partners and shared services.

The actionable requirement is to specify acceptable response, degradation and restoration targets for each critical workflow, and to identify which network and third-party components can affect those targets.

Match service requirements to the transaction, not a generic speed claim

Financial networks carry workloads with different performance profiles. A branch employee opening a customer record needs dependable application response; a payment gateway needs reliable processing and exception handling; analytics platforms may be more sensitive to throughput or data-transfer windows. Specialist electronic trading can have exceptionally tight latency constraints, but those should not be generalized to retail banking, insurance or wealth management.

Sub-millisecond network design may be appropriate for particular trading locations and applications, but it is not a universal benchmark for enterprise financial connectivity. Service objectives should reflect the application, geography, available routes, end-to-end architecture and operational consequences of delay.

Those objectives should also define unacceptable degradation, dependency ownership, visibility across network and application layers and tested alternatives during disruption. Network investment can then be discussed in terms of service outcomes rather than purchased capacity alone.

Readiness for API-led ecosystems is another dependency question

A separate question in our opinion analysis classified **69% of discussions** as indicating that connectivity was mostly ready for open-banking APIs, **23%** as not ready and 7% as not currently prioritizing API readiness. These are inferred assessments, not an audit of API security or operational readiness. Their relevance internationally is the need to understand dependencies across customer-consented data sharing and partner ecosystems, which differ by jurisdiction.

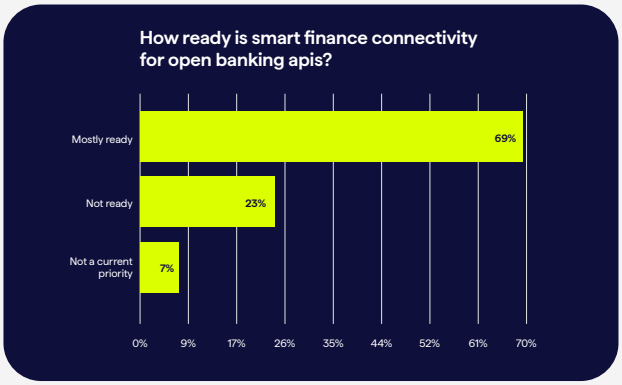


Figure 2. Perceived readiness for open-banking APIs. Categories are not audited readiness levels.

API readiness extends beyond publishing an endpoint. Service owners need to consider identity and consent controls, application gateways, routing, cloud availability and dependencies on partners and upstream data services.

The priorities will differ between markets with established open-banking requirements and those at earlier stages of API-enabled financial services. Organizations should map applicable rules and critical services before assuming that a favorable perception of readiness guarantees production resilience.

API availability may depend on authentication, application gateways, cloud connectivity, upstream data services and partner infrastructure. A reachable endpoint is not sufficient if transaction completion or data integrity is degraded elsewhere in the service chain. Network teams should therefore work alongside application and security owners to define the critical end-to-end pathways that need measurable assurance.

Strategic insight

Always-on finance requires network performance to be defined by the critical services and customer outcomes it supports, not by an undifferentiated promise of speed or availability.

As payment activity and connected services expand, financial institutions need explicit network requirements reflecting transaction patterns, partner dependencies and recovery needs. This provides the foundation for the next challenge: demonstrating that important financial services can withstand disruption and be restored reliably.

Expereo perspective:

Buy for the workload, not the headline speed

A payment request, a branch application and a scheduled data transfer have different network requirements. Those differences matter most during disruption. A backup connection may be working but lack the capacity to carry essential services at peak demand. Network design needs to establish which transactions take priority, what delay is acceptable and how the service behaves when capacity is reduced. Testing must show that the transaction still completes.

Julian Skeels
Chief Digital Officer, Expereo



Theme 2:

From network availability to operational resilience

A connected system is not necessarily a dependable financial service.

A connection can report that it is operational while a financial application is slow, a remote user cannot authenticate, or a payment dependency is unreachable. A brief interruption may have very different consequences depending on the affected service and whether traffic can be rerouted or functionality restored. Circuit availability remains necessary, but it is not a complete measure of operational resilience.

For institutions with distributed offices and external technology dependencies, faults can arise in access networks, security controls, cloud regions, application providers or integrations beyond their direct control. If each layer is monitored and managed separately, locating the source of degraded service may take longer than the underlying technical repair.

Critical-service assurance needs more than an uptime figure

A contracted availability percentage is only one element of service assurance. The Basel Committee on Banking Supervision sets out principles for banks to identify critical operations, understand interdependencies and build the capacity to withstand and recover from disruption. The central question is what continuity each important financial service requires and how failures across its supporting chain will be tested.

This approach is relevant across markets, although detailed obligations vary. Business continuity programs should connect technology recovery with business operations, incident communication, scenario testing and accountability. Restoring a circuit does not necessarily mean that a payment, branch or customer service has returned to an acceptable operating state.

A disciplined assessment starts with service impact. Which customer journeys or internal processes would be affected if a branch lost access to the core platform? Can a payment service still operate if one data feed is unavailable? Does an alternative path depend on the same physical access route or third-party gateway? These questions make dependencies visible before an incident tests them.

Service assurance chain: Illustrative operating framework, not survey data



Figure 3. Illustrative service-assurance chain: a practical discussion framework, not research data or a prescribed regulatory model.

Third-party dependencies can amplify disruption

The Financial Stability Board's global third-party risk toolkit identifies the importance of critical service dependencies across outsourcing and technology providers. In the EU, the Digital Operational Resilience Act (DORA) adds specific ICT risk-management, testing and third-party oversight requirements for institutions within its scope. These sources have different status and geographic coverage, but both reinforce the need to examine the complete service chain.



A financial institution may depend on a local carrier, a global WAN partner, a cloud security platform and a hosted application for one business-critical service. An effective operating model establishes the role of each provider, the practical recovery path and the evidence needed for diagnosis. Multiple contracts do not automatically amount to a coherent operational view.

Diversity must be tested rather than assumed. Two access providers can share a physical building entry, duct route or upstream dependency. Cloud failover may still depend on a single identity, DNS or connectivity layer. Decisions about resilience should be based on service criticality and verified failure scenarios, not a blanket prescription for maximum redundancy at every site.

Measure recovery in business terms

Connectivity leaders can make resilience more tangible through a small set of agreed measures: application reachability, performance against service-specific baselines, time to identify the fault domain, time to restore business functionality, recurrence of incidents and the completeness of recovery tests. The most useful dashboard explains what happened to an important service and what action follows, rather than merely displaying a collection of green infrastructure indicators.

The supporting operating model should define how network operations, application owners, security teams, business continuity specialists and external suppliers coordinate during an incident. Post-incident reviews should identify whether the service failed because of missing visibility, unclear escalation, inadequate redundancy or a dependency outside the expected recovery design. That diagnosis can guide investment more reliably than an aggregate uptime figure alone.

Strategic insight

Operational resilience is demonstrated through tested service continuity, clear incident attribution and accountable recovery, not solely through contractual availability commitments.

Financial institutions need to connect network monitoring to the services they must protect, and give internal and external teams a common basis for action when performance declines. Achieving this across regions and business lines depends on coordinated operating models for hybrid architecture and third-party services.

Expereo perspective:

“

The hardest incidents are the ones where everyone is technically right. The carrier sees a healthy circuit, the cloud provider shows green, the application team finds nothing in its logs, and a branch still can't reach the core platform. Most of the lost time goes on proving whose problem it is. As a single point of contact across providers, we take that question off the customer's desk. Under DORA and similar regimes, what counts is how quickly the service comes back, not how quickly each ticket closes.

”

Julian Skeels
Chief Digital Officer,
Expereo



Theme 3:
Managing complexity across hybrid financial infrastructure

Hybrid operations create value when connectivity, visibility and supplier accountability are coordinated.

Financial institutions rarely run every application from one environment. Branches, regional offices, private data centers, cloud platforms and third-party services may all form part of a customer or employee journey. Architecture must reflect service needs, data responsibilities, resilience choices and regional connectivity conditions rather than a fashionable deployment model.

Hybrid architectures can fragment accountability. A user may experience degradation while the carrier reports a healthy circuit, the cloud provider reports availability and an application team sees no isolated fault. Without comparable telemetry and shared ownership, each statement can be accurate without explaining why the financial service is underperforming.

Hybrid-cloud preferences point to diverse operating needs

In our opinion analysis, **37% of classifications viewed** hybrid cloud positively for connectivity, while **26%** viewed mostly on-premises environments favorably and 11% viewed private cloud favorably. These are selected perceptions from different categories, not mutually exclusive deployment shares or a survey of global infrastructure estates.

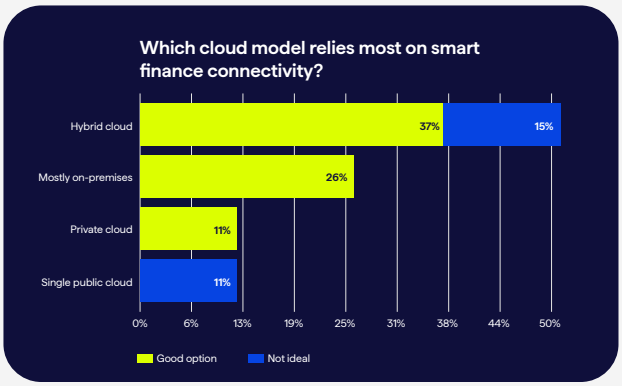


Figure 4. Cloud arrangements and connectivity in financial-services discussions; the categories are not market shares.

The practical significance of these preferences is diversity. Financial institutions may retain core systems in private or on-premises environments while using public cloud for digital channels, analytics or selected applications. Different workloads generate different network access, security, data-location and recovery requirements; no single hosting architecture is automatically optimal for every institution.

Hybrid services create value when the connections between environments can be understood and managed. This means mapping important application paths, establishing measurable performance targets and providing a consistent approach to incident ownership, regardless of where a workload is hosted.

Concentration risk can arise when critical workloads depend on a common provider, control plane or location. Equally, spreading services across multiple clouds adds integration and management overhead. The relevant choice is a tested architecture aligned with service criticality, not an assumption that any one cloud model is inherently safe or unsafe.

Coordinated service management matters more than carrier uniformity

The practical question for a multi-site financial institution is how global and local connectivity is procured, documented, monitored, changed and restored. Different regions may benefit from different Internet access suppliers, routing options or local support arrangements. Supplier diversity can improve coverage and resilience, but only if the institution can maintain coherent oversight of the resulting services.

The Financial Stability Board's third-party risk toolkit describes a flexible, risk-based approach to identifying critical third-party services and managing dependencies throughout the relationship lifecycle. For network leaders, this means retaining clear ownership of services and performance even when delivery spans local carriers, global network partners and cloud platforms.

A coordinated view of incidents, service locations, circuit ownership, contacts, performance baselines and planned changes enables faster escalation and clearer prioritization. It also reduces the need for central teams to reconstruct basic service information each time a fault occurs, or a new site is connected. Consistent processes can therefore deliver value without requiring every location to use identical access technologies.

Managing complexity across hybrid financial infrastructure

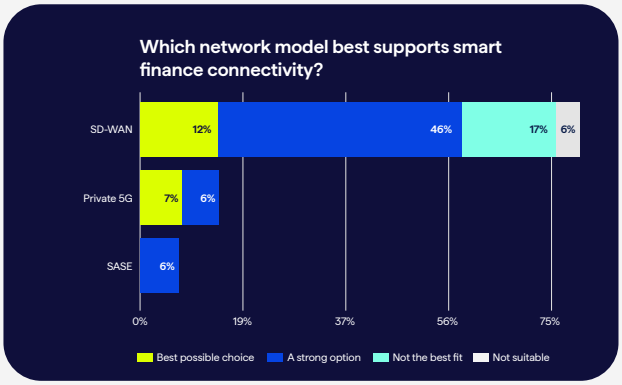


Figure 5. Perceptions of SD-WAN, private 5G and SASE. The technologies have different functions; bar lengths are not comparable market shares.

The evaluation should start with the workload. Application-aware routing may help traffic move across available paths; central management can support more consistent branch operations; secure access controls matter for distributed users and partners. Product selection alone does not demonstrate that a service is resilient, accountable or appropriate for local regulatory obligations.



Strategic insight

Hybrid financial connectivity delivers value when different infrastructure choices operate within one accountable service-management model, not when every site adopts the same technology.

The priority is consistent service requirements, cross-provider visibility, coordinated incidents and transparent ownership across a technically diverse estate. Those foundations also help institutions manage the security and governance obligations of increasingly connected financial ecosystems.

Expereo perspective:

Carrier choice is local, accountability is global

Supplier diversity is great for resilience until nobody can see the whole picture. A global bank might run local ISPs in dozens of markets, two clouds and a SASE platform, each with its own portal and its own idea of normal. You should be free to pick the right access and provider for each location, as long as it all sits inside one operating model with one inventory and one escalation path. That's the job of the Expereo platform. Treat carrier choice as a local decision and accountability as a global one.

Matthew Lea
Product Development Director, Expereo



Theme 4:

Security and trust across connected financial ecosystems

Secure finance depends on appropriate controls, shared accountability and forward-looking risk management.

Financial-services security must accommodate employees, customers, partners, cloud systems and external providers accessing sensitive data and critical applications. As connectivity reaches across those environments, network design and security controls become harder to govern independently. A service may be available but overexposed; it may also be strongly restricted yet operationally fragile during an incident.

Security must therefore sit alongside continuity and service ownership. Appropriate controls depend on the resource, data sensitivity, identity, device and access path. Organizations also need to know who manages exceptions, how policy changes are tested, which audit evidence is retained and how critical access is preserved during containment and recovery.

Zero trust is a security principle, not a substitute for network design

In our opinion analysis, 55% of classifications viewed zero trust as a foundational security approach and another 33% as a strong basis. These are inferred views, not audited evidence of completed deployments. The separate SASE category should not be treated as a competing choice; SASE capabilities can be used to help implement zero-trust principles.

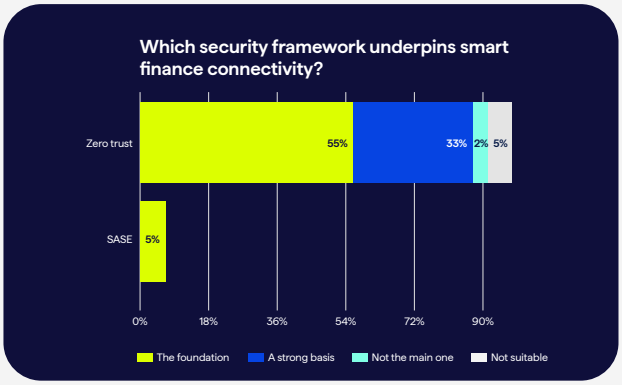


Figure 6. Views of zero trust and SASE in US financial-services discussions; these are not equivalent security classifications.

NIST SP 800-207 describes zero trust as an approach centered on users, resources and context rather than assumed trust based on network location. This is useful for distributed finance, where employees and third parties access sensitive applications from different locations and networks. It does not remove the need for strong architecture, identity governance, availability planning and operational testing.

Security architecture and network reliability must be designed together. For example, changes to access policies, identity dependencies or security inspection paths need the same change discipline and recovery planning as changes to a core network route. A control is effective only if legitimate critical services can continue to operate safely.

Regulatory requirements vary across financial subsectors

There is no single global compliance regime for financial connectivity. Institutions should map regulatory and contractual obligations to their legal entities, customers, activities and data. EU DORA applies to a defined range of financial entities and ICT third-party arrangements, while other markets have their own resilience, cybersecurity and outsourcing requirements.

Regardless of jurisdiction, a multi-provider operating model should identify who controls information and access, who can act during an incident and how governance evidence is retained. This is particularly important when financial institutions depend on managed networks, cloud platforms and external technology partners.

Post-quantum readiness is a planning question now

Our opinion analysis classified 69% of discussions as acknowledging post-quantum security but not acting, and 31% as not yet considering it. These are directional perceptions, not audited cryptographic inventories or reliable adoption percentages. The strategic concern is nevertheless relevant worldwide wherever institutions retain long-lived sensitive data or depend on systems that may need cryptographic migration.

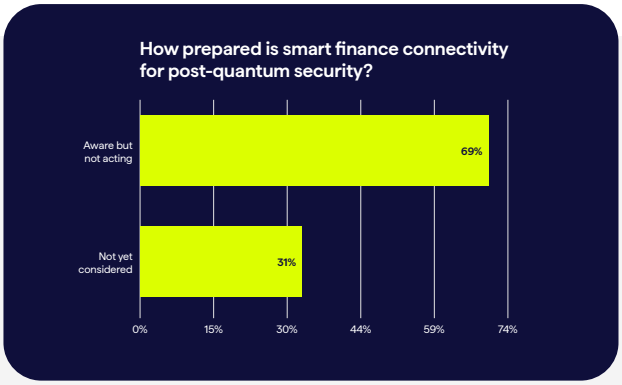


Figure 7. Discussion about post-quantum planning; not a verified measure of global readiness.

Strategic insight

Trustworthy financial connectivity depends on secure, recoverable services and clearly assigned responsibilities across users, institutions and suppliers, rather than reliance on one security label.

Security choices should reinforce continuity, meet applicable jurisdictional expectations and remain adaptable as threats and standards evolve. These foundations also support the more data-intensive and potentially automated financial services that network teams increasingly need to enable.

NIST finalized its first three post-quantum cryptography standards in August 2024 and has encouraged organizations to begin planning transitions. For financial institutions, the practical starting point is an inventory of cryptography used in high-value applications, connectivity components and third-party services, together with an assessment of information longevity and replacement complexity.

Migration planning must account for interoperability, supplier readiness, testing and staged implementation. Different jurisdictions and regulators may set specific expectations, but the technical challenge spans global networks and service providers. Institutions should avoid assuming that replacing a single network device or security product resolves the entire dependency chain.

For network leaders, the important question is therefore not whether quantum computing will transform finance immediately, but whether cryptographic dependencies are understood well enough to plan an orderly transition as standards and threats evolve.

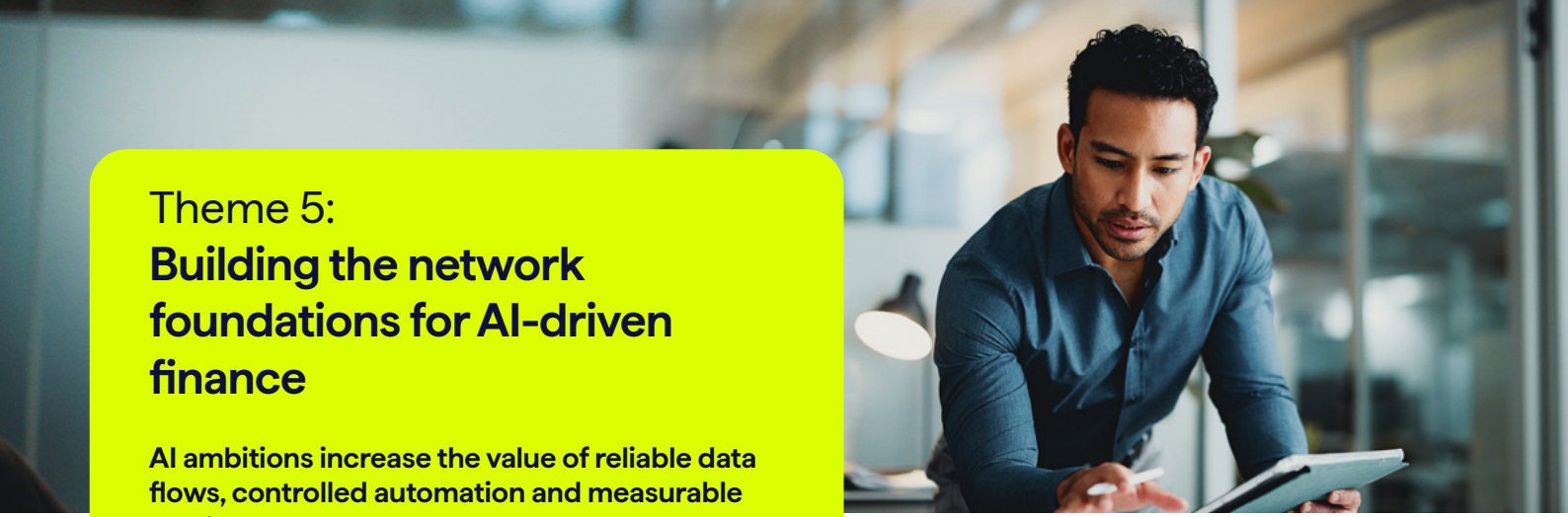
Expereo perspective:

Every security control is also a dependency

Every security control is also a dependency. Add an inspection point or tighten an identity policy and you've changed the path a payment takes, so that change deserves the same testing and rollback plan as a core routing change. Post-quantum cryptography will stretch this further than anything before it. It touches network devices, SASE services and third-party links at once, and no single product swap covers it. Institutions that start their cryptographic inventory now get to migrate on their own timetable instead of someone else's.

Jean-Philippe Avelange
Chief Information Officer, Expereo





Theme 5: Building the network foundations for AI-driven finance

AI ambitions increase the value of reliable data flows, controlled automation and measurable service outcomes.

AI already supports varied financial-services functions, from customer interactions and risk analysis to fraud monitoring and trading. Their connectivity needs differ: some workloads exchange large datasets with compute platforms, others rely on timely event streams, and customer-facing applications may need predictable responses across regions. Planning must distinguish wider AI use in finance from the narrower use of AI to manage networks.

A financial institution can deploy AI-enabled products while network troubleshooting remains fragmented across carriers, cloud infrastructure and security systems. Conversely, operational automation can improve diagnosis and service quality without the organization adopting autonomous AI operations. These are different capabilities with different risks and measures of success.

Separate strategic ambition from network-operation deployment

Our opinion analysis classified 64% of discussions as identifying AI and data workload readiness as a top connectivity priority for 2027, with a further 18% treating it as important. These are forward-looking perceptions, not evidence that the required networks, data platforms or controls have been deployed.

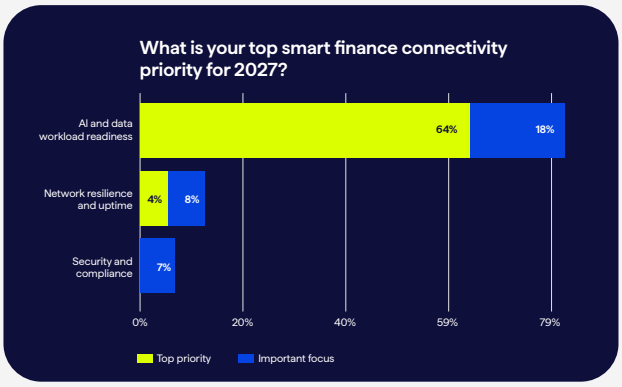


Figure 8. 2027 connectivity priorities, including AI/data readiness, resilience and security. The figures represent inferred discussion classifications

AI is already present in financial services, but applying AI directly to network operations is a narrower question. We have not treated near-universal non-adoption classifications from online discussions as evidence of actual industry deployment levels; a robust comparison would require clearly defined questions and audited organizational data.

The Financial Stability Board's research on AI in finance describes a widening range of use cases alongside vulnerabilities relating to third-party dependencies, cyber risk, model governance and data quality. These findings apply across member jurisdictions and provide stronger context for the operating controls institutions need than a single modeled adoption headline.

For network leaders, the essential distinction is between investment ambition, the requirements of AI workloads and the maturity of AI-assisted network operations. Each has different information requirements, security responsibilities and evidence of business value.

The BIS Financial Stability Institute's 2026 work on AI data in finance highlights privacy, quality, security and third-party dependencies as barriers to trustworthy deployment. These considerations are especially pertinent when network teams need to understand where data travels, which platforms process it and whether performance or security boundaries can be reliably observed.

The analysis also contained minority classifications prioritizing resilience or security. Rather than treat these as evidence that such concerns are unimportant elsewhere, the practical interpretation is that AI readiness needs to be developed alongside existing obligations for continuity, cybersecurity and sound service management.



AI workloads create distinct network assurance requirements

Our opinion analysis classified 65% of discussions as associating AI-driven risk modeling with some connectivity strain and 24% with minor strain. The classification does not measure network utilization or define consistent workloads. It does, however, raise a practical need for application-aware capacity planning where models access distributed datasets or cloud compute.

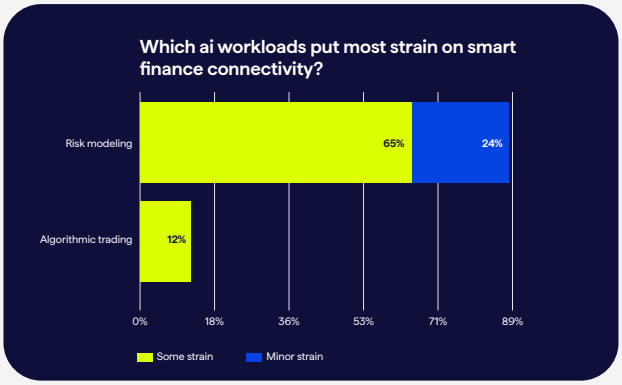


Figure 9. Views of relative connectivity demands from risk modeling and algorithmic trading; not measured throughput.

The degree of network pressure depends on workload design. A model that periodically transfers a large dataset may be more sensitive to throughput and transfer windows; a continuous fraud signal may require low variability in event delivery. Neither maps neatly to a single generic category of AI network demand.

Institutions should therefore assess data locations, movement patterns, sensitivity, processing timeframes and dependencies on external platforms. The useful question is how network design supports a given business process, not how much strain an undifferentiated AI category supposedly creates.

One institution may prioritize predictable overnight transfers; another may depend on continuously available fraud-event feeds; a third may focus on access to cloud-hosted customer applications. These distinctions affect routing, monitoring, change controls and recovery planning, and they prevent an overly narrow approach to AI connectivity.

The assessment should link those workload profiles to measurable network objectives and clear visibility across application, cloud and provider boundaries, especially where an institution does not manage every component of a critical path.

Operational intelligence needs trustworthy data and clear control

AI-assisted network operations may help identify recurring performance anomalies, group related alerts or suggest likely fault domains. But automation depends on accurate inventory data, comparable telemetry, usable incident records and a reliable understanding of which services support important financial processes. Poor-quality data can produce plausible but misleading recommendations or cause an automated response to focus on the wrong component.

The NIST AI Risk Management Framework offers a useful reference through its Govern, Map, Measure and Manage functions. For network operations, the implication is to define the purpose of AI-assisted actions, establish who checks the results, set acceptable performance thresholds and specify how errors or unintended effects will be detected and corrected.

A prudent sequence begins with decision support, not unbounded autonomy. Teams can test AI-assisted diagnostics against historical incidents, evaluate false positives, verify likely causes and introduce tightly scoped actions such as ticket enrichment or approved routing recommendations. More consequential changes should operate within clear policy limits, change windows where appropriate, human approval thresholds and reversible processes.

Responsibility also needs to extend across suppliers. If a managed network partner introduces automated traffic optimization, the institution should understand what is being optimized, what telemetry informs decisions and what happens when performance targets are missed. The outcome to measure is improved service quality or shorter, safer incident resolution, not simply the number of AI features activated.

Strategic insight

AI-ready financial networking is demonstrated through dependable service performance, trustworthy operational information and governed decisions, not by the number of AI tools deployed.

Financial leaders should connect AI workload planning to measurable application requirements, then apply appropriate oversight and resilience controls to operational automation. Across the five themes, the same requirement emerges: financial connectivity must be visible, secure, recoverable and continuously improved in the context of the services it enables.

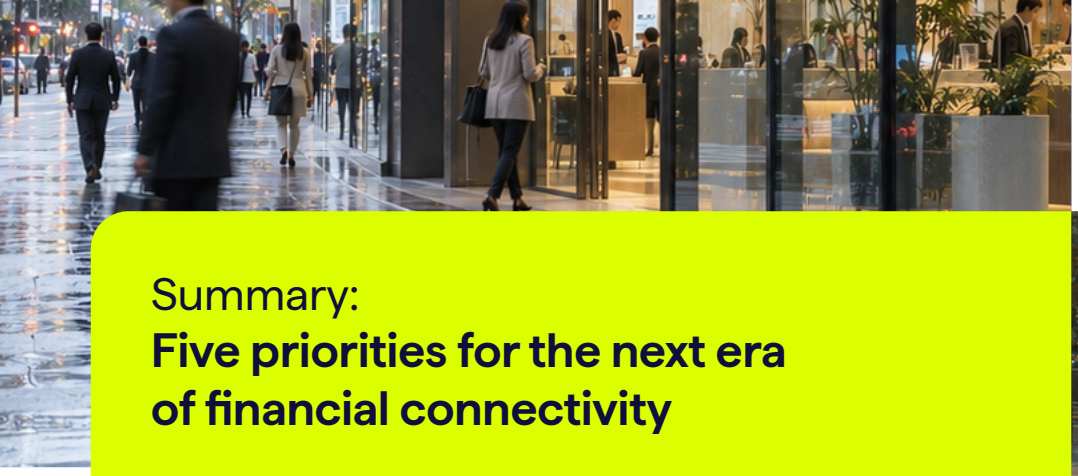
Expereo perspective:

There is no such thing as generic AI traffic

For live fraud checks, a model's accuracy is only useful if its decision arrives in time to support the transaction. The network requirement depends on where the model runs and which data it needs. If that response is late or unavailable, the institution needs an agreed policy for continuing, holding or declining the transaction. Network design and failure testing must support that policy. More bandwidth alone cannot resolve those choices.

Julian Skeels
Chief Digital Officer, Expereo







Summary:
Five priorities for the next era of financial connectivity

Turning real-time financial ambition into measurable, resilient and secure operations

Five connected priorities emerge from the research, highlighting the capabilities financial institutions need to sustain always-on services across complex digital estates.

1 Translate critical service requirements into network objectives

Define what key payment, customer, branch and data workflows need from connectivity. Set appropriate performance and recovery requirements for each, identify external dependencies and avoid applying specialist trading latency criteria to unrelated workloads.

2 Make operational resilience visible and testable

Monitor service quality as well as circuit status, connect incidents to business impact and test recovery across the actual network, security, application and provider chain. The aim is to restore important financial functions, not merely individual technical components.

3 Coordinate hybrid connectivity and third-party service ownership

Maintain consistent visibility of locations, suppliers, policies, changes and escalation routes across different access technologies and cloud models. Clear accountability is more valuable than a uniform architecture that ignores local or workload-specific requirements.

4 Treat secure access and regulatory preparedness as ongoing operations

Apply security controls according to identity, resources and risk; connect supplier oversight to incident response; and develop a manageable plan for emerging cryptographic standards. The requirements must reflect the institution and services actually regulated.

5 Build AI readiness on dependable data and governed automation

Plan for the data movement and service characteristics of real AI workloads. Introduce operational AI only where there are reliable inputs, measurable results, engineering oversight and safe boundaries for automated action.

Together, these priorities form a practical basis for evaluating financial network readiness and deciding where targeted improvements are likely to deliver the greatest operational value.



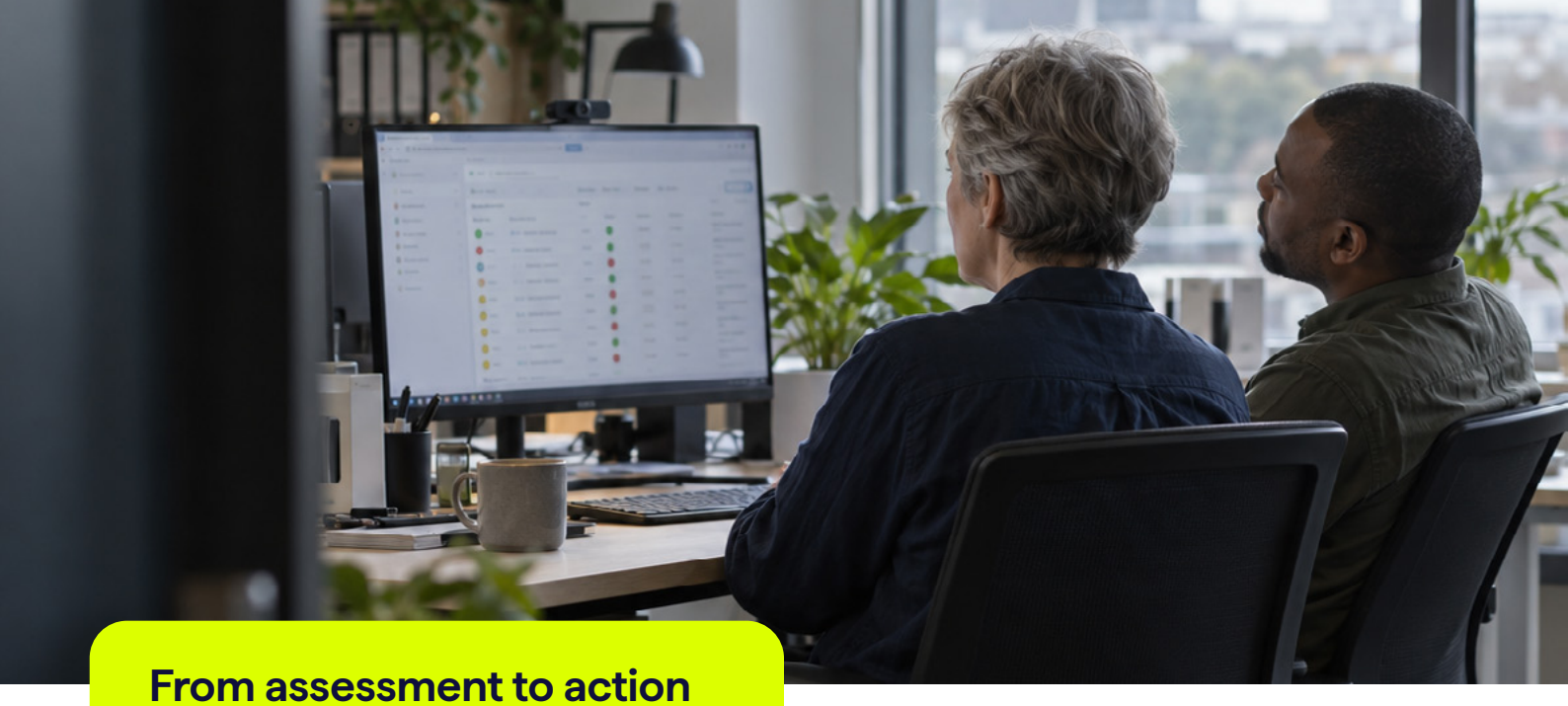
Financial Network Resilience and Readiness Scorecard

A practical, qualitative assessment for distributed financial-services organizations.

The six-dimension scorecard translates the report into a discussion tool for CIOs, infrastructure leaders and service owners. It is an editorial framework derived from the research themes, not a statistically validated industry maturity benchmark. Assess existing, demonstrable capabilities rather than aspirational roadmaps.

Dimension	Developing	Established	Advanced
1. Transaction-critical performance	Circuit health is tracked; the effect on critical applications and transactions is uncertain.	Important services have work-load-specific baselines, alerts and named performance own-ers.	End-to-end service measures link network quality to transaction completion, user out-comes and improvement.
2. Continuity and recovery	Recovery relies on individual technical teams; dependencies and restoration objectives are incomplete.	Critical dependencies, restoration roles and escalation paths are documented and tested.	Scenario testing and incident reviews demonstrate recovery of financial services across suppliers.
3. Hybrid and cloud connectivity	Cloud, branch and provider services are monitored separately; service ownership is fragmented.	Core paths, access services and service ownership are visible through common processes.	Cross-provider service intelli-gence supports proactive diagnosis, optimization and planned change.
4. Security and governance	Controls and access policies vary; third-party and incident responsibilities are unclear.	Risk-based access, incident procedures and supplier responsibilities are defined and reviewed.	Security, resilience and evidence obligations are integrated into ongoing changes and recovery testing.
5. Provider coordination	Carrier inventories, contracts, support paths and incident records sit in silos.	Central teams can identify service owners, providers, perfor-mance and escalation contacts.	Different providers operate within a coherent lifecycle of service assurance, reporting and improvement.
6. AI and data readiness	AI demand and network auto-mation are discussed without measurable workload needs or trusted telemetry.	Priority data flows are mapped, telemetry is reliable and selected automation is governed.	AI-assisted decisions are evaluated for safety, service improvement and measurable business value.

Framework note: A qualitative self-assessment developed from the report themes. These categories are not research sample statistics or a statistically validated maturity benchmark; assess demonstrated practices rather than planned capabilities.



From assessment to action

A readiness scorecard is useful when it informs real decisions. Institutions should prioritize gaps according to the importance of the services affected rather than trying to score "advanced" on every dimension. A branch-heavy bank might focus on application dependencies, a global asset manager on supplier coordination, and a payments provider on recovery testing across its full-service chain.

Use the following three-step review to translate the assessment into action, then revisit the scorecard after material changes to the estate or service requirements:

- **Prioritize business-critical services.** Identify the journeys, transactions and data flows whose disruption creates the greatest customer, operational or regulatory exposure.
- **Validate the evidence and dependencies.** Review performance baselines, service ownership, recovery routes, third-party arrangements and the actual results of incident tests.
- **Assign owners and revisit progress.** Agree targeted improvements across network, cloud, security, applications and suppliers; reassess as workloads or material dependencies change.

Strategic outlook: From connected services to assured finance

Financial-services transformation will create different network demands at once. Fast payments require dependable access to transaction services; hybrid cloud adds distributed dependencies; security and cryptographic standards continue to evolve; and AI increases the importance of trusted data movement and governed change. None of these pressures can be addressed by connectivity speed alone.

Institutions best positioned to respond will establish a shared understanding of critical services, measure how network conditions affect them and coordinate the internal teams and suppliers involved in normal operations and incident recovery. They will distinguish specialist low-latency applications from workloads for which continuity, application visibility or managed multi-provider complexity is more valuable.

For Expereo, the relevant contribution is helping global institutions manage complex network estates through coordinated connectivity services, improved application experience and clearer operational visibility. Such support should be assessed against each institution's needs and responsibilities, not confused with direct control of payments platforms or regulatory compliance programs.

The future of financial connectivity is not simply a faster network. It is confidence that important services can continue, recover and improve as digital finance evolves.

Closing perspective

Be the partner who calls when providers point at each other

Finance will soon run on more providers, more jurisdictions and more automation than any one team can hold in its head. Confidence comes from knowing, at any moment, which services matter, who owns each dependency and how fast you can recover. We're clear about where our role stops: we don't run payment platforms or compliance programs. What we do is make the network predictable across up to 190 countries, give you one view of it, and pick up the phone when two other providers are pointing at each other.

Jean-Philippe Avelange
Chief Information Officer,
Expereo



Continue the conversation

The scorecard offers a starting point for assessing where network visibility, coordination or resilience improvements could make the greatest difference. To discuss global connectivity and managed network priorities for financial services, visit Expereo

[Nominated Expereo contact: full name and job title]

[LinkedIn profile, if required]

[Contact email, if required]

Visit Expereo