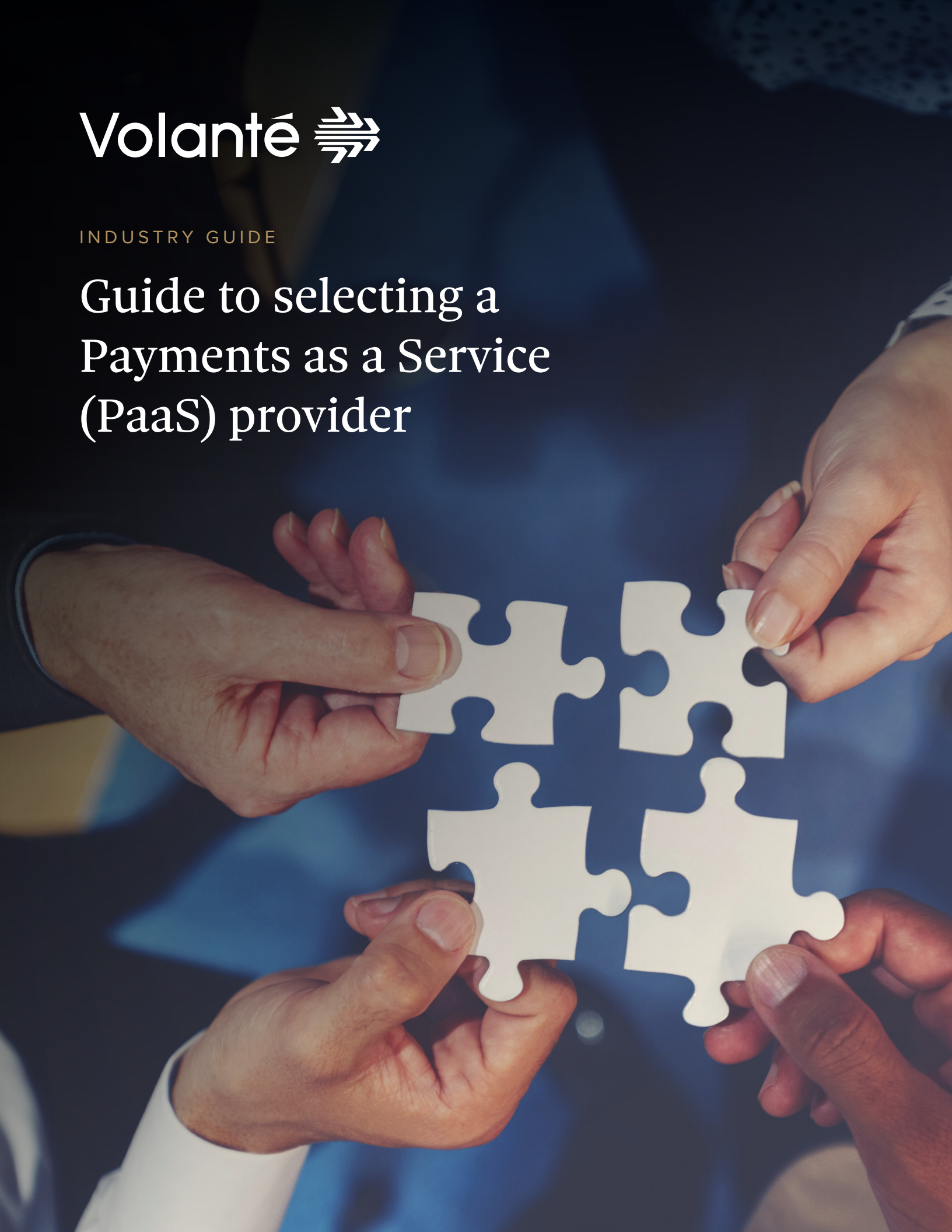




INDUSTRY GUIDE

# Guide to selecting a Payments as a Service (PaaS) provider



# Table of contents

The payments modernization challenge	2
The case for payments as a service (PaaS)	2
Purpose of this guide	2
Moving from an on-premise model	
to a cloud-based PaaS model	3
The 6 key success factors for PaaS selection	4
Evaluation framework and provider assessment	5
Corporate overview	6
Financial position	8
Market position	7
Core platform assessment	9
Real-time payments	10
RTGS and high-value payments	11
Low-value and bulk payments	12
Cross-border and SWIFT payments	13
Payment schemes and rails	14
ISO 20022 migration and standards	15
Architecture and deployment	16
Integration capabilities	17
Configurability and self-service	18
Security architecture	19
PaaS vendor security checklist	20
Regulatory compliance	22
Product roadmap	23
Onboarding, training, and support	24
Pricing structure	25
Conclusion: Moving forward with PaaS provider selection	26



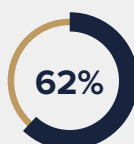
## The payment modernization challenge

Financial institutions face mounting challenges in modernizing their payment infrastructure, from complex operations to evolving regulatory demands. Banks must handle different payment types and channels across regions while managing growing transaction volumes and customer expectations for real-time processing. This urgency is reflected in market data showing 100% of mid-tier banks planning at least moderate payment technology investments over the next 24-36 months.<sup>1</sup>

The requirement to support new payment schemes and implement standards like ISO 20022 adds to the challenge—with 62% of mid-tier bank customers already using or planning to use these messaging formats.<sup>2</sup> Banks must also balance operational costs, maintain legacy systems, manage transaction fees, and ensure compliance with data privacy and security standards across jurisdictions. Yet, banks are not seeing commensurate increases in budgets and staff. Banks are increasingly turning to Payments as a Service (PaaS) solutions to solve this dilemma.



of mid-tier banks planning at least moderate payment technology investments over the next 24-36 months.<sup>1</sup>

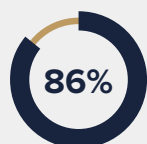


of mid-tier bank customers already using or planning to use these messaging formats.<sup>2</sup>

## The case for Payments as a Service (PaaS)

Payments as a Service (PaaS) represents a modern approach to payment processing, leveraging cloud technology to deliver core payment capabilities with significant advantages over traditional infrastructure. This transition is already well underway, with 86% of mid-tier banks preferring hybrid cloud approaches for their payment operations.<sup>3</sup> PaaS enables banks to reduce operational complexity and launch new services faster—crucial given that 59% of mid-tier bank customers expect to increase their usage of real-time payments in the next 12 months.<sup>4</sup>

The financial benefits are equally compelling: PaaS requires less upfront investment than traditional systems, offers more predictable operating costs through subscription pricing, and reduces maintenance costs through its pay-per-use model. While these advantages are clear, selecting the right provider requires careful consideration and a structured approach.



of mid-tier banks preferring hybrid cloud approaches for their payment operations.<sup>3</sup>



of mid-tier bank customers expect to increase their usage of real-time payments in the next 12 months.<sup>4</sup>

## Purpose of this guide

This guide serves as a comprehensive resource for financial institutions embarking on their payments modernization journey. It provides a structured framework and questionnaire for evaluating potential PaaS providers. Through detailed analysis and clear methodologies, this guide helps organizations navigate the selection process with confidence and make informed decisions based on their specific needs.

<sup>1-4</sup> Volante Technologies - [Payments as a Service: A fast track to payments modernization](#)



# Moving from an on-premise model to a cloud-based PaaS model

The transition from traditional on-premise payment systems to a cloud-based Payments as a Service (PaaS) solution requires careful consideration across several dimensions:

- **Architecture and infrastructure:** PaaS providers take on responsibility for managing the underlying payment infrastructure, including servers, networks, and capacity planning, while banks maintain focus on core banking integration. During transition, banks typically operate in a hybrid model until migration is complete.
- **Data management:** Banks must develop comprehensive migration strategies that address both data volume and sensitivity, while maintaining system availability throughout the transition. The shift to PaaS introduces new considerations around data residency and sovereignty, requiring careful planning around governance frameworks and controls.
- **Security and compliance:** Leading PaaS providers deploy solutions on major cloud platforms that often exceed security capabilities achievable with private infrastructure. While providers handle much of the security and compliance management, banks must still perform thorough due diligence and maintain oversight of provider certifications and frameworks.
- **Operational impact:** Staff roles shift from infrastructure management to higher-value activities like payment strategy and client service, requiring clear communication about changing responsibilities. Service level agreements become crucial in defining provider responsibilities and establishing effective vendor management practices.
- **Risk management:** Banks transfer many operational and technical risks to the provider but must develop robust oversight capabilities and vendor risk management practices. Contingency planning focuses on scenarios like provider disruptions, requiring contracts with clear service commitments and data portability provisions.
- **Cost implications:** The financial model shifts from capital-intensive infrastructure investments to a predictable operational expense model based on transaction volumes or usage. This typically reduces total cost of ownership by eliminating hidden costs of maintaining payment infrastructure in-house, though banks must carefully evaluate provider pricing structures.



**Accenture**, a global leader in digital transformation and banking innovation, specializing in Payments as a Service (PaaS), helps financial institutions modernize and optimize their payment operations. They agree that selecting your PaaS provider should be a trusted strategic partner.

**Bhaskar Banerjee, Principal Director, Accenture**

*"Payments as a Service (PaaS) is not a new concept, but in today's dynamic world of payments, it has become a critical enabler of security, scalability, agility, and seamless integration. The right PaaS provider is not just a vendor—it's a strategic partner that aligns with FI's vision for the future of payment modernization. Choosing the ideal partner is not just about the technology. Rather, it requires a balance of technical expertise, financial stability, and a commitment to driving transformative change."*

## The 6 key success factors every PaaS selection process should have in place

- 1 Executive sponsorship and governance:** Secure active engagement from senior leadership who can remove obstacles and establish clear decision-making frameworks.
- 2 Stakeholder engagement:** Ensure participation from all relevant teams (operations, technology, risk, compliance, finance, and business units) with clear communication channels for feedback and concerns.
- 3 Requirements clarity:** Develop clear requirements encompassing functional, technical, operational, compliance, and scalability needs, but avoid customizing vendor solutions to match current processes.
- 4 Risk management:** Maintain a systematic approach to identifying and mitigating risks throughout the selection process, from vendor evaluation through implementation planning.
- 5 Change management:** Begin early with comprehensive training programs and clear communication about evolving roles and responsibilities to ensure staff understanding and support for the transition.
- 6 Implementation planning:** Consider implementation requirements early in the selection process, including resource needs, integration challenges, and operational transitions to ensure readiness for deployment.



## Evaluation framework and provider assessment

This guide provides a structured framework for evaluating potential PaaS providers across seven assessment areas. The framework is designed to be both thorough and flexible, allowing organizations to adapt the evaluation criteria based on their unique requirements while maintaining consistent assessment standards.

- |          |   |          |  |
|----------|---|----------|--|
| <b>1</b> | <b>Corporate overview:</b> Evaluates organizational foundation, stability, and commitment to payments | <b>5</b> | <b>Technical implementation and integration:</b> Evaluates implementation ability and integration approaches |
| <b>2</b> | <b>Financial position:</b> Assesses ability to sustain investment and support innovation              | <b>6</b> | <b>Security and compliance:</b> Examines security controls and regulatory compliance capabilities            |
| <b>3</b> | <b>Market position:</b> Examines competitive strengths and strategic direction                        | <b>7</b> | <b>Innovation and future development:</b> Assesses product roadmap and commitment to evolution               |
| <b>4</b> | <b>Core platform assessment:</b> Reviews technical capabilities and architecture                      |          |  |





## Corporate overview

### Why this is important

A provider's corporate foundation and stability are crucial indicators of their ability to support your long-term payment modernization journey. With vast majority of banks planning significant payment technology investments, you need a stable partner with proven commitment to the payments market who can support your transformation while continuing to innovate. Their organizational structure and market focus directly impact their ability to deliver reliable service and maintain investment in payment capabilities that align with your needs.

### What to look for in a PaaS provider

- The provider generates at least 75% of their revenue from payments and PaaS solutions, indicating strong focus and continued investment in the roadmap
- Core product team consists of more than 80% full-time employees vs. contractors, ensuring continuity and knowledge retention during implementation and beyond
- Minimum five years of experience providing PaaS solutions with proven delivery capabilities in your region
- Ability to provide responsive support aligned with your region and time zones
- Track record of innovation in payments and release of new service and offerings, showing strength of roadmap aligned with customer needs
- Established partnerships with major cloud providers and payment networks, indicating strong ecosystem relationships that benefit customers

### Introductory questions

1. What is the location of your company headquarters (city/country)?
2. In which year was your company founded?
3. What is your company's ownership structure (public vs. private)?
4. Please elaborate on your company's organizational structure, specifically detailing which business unit is responsible for payment solutions.
5. Please describe innovations and new product releases in the last three years that relate to your PaaS offering.



## Financial position

### Why this is important

Financial stability underpins a provider's ability to invest in innovation and maintain service quality. The payments industry demands continuous investment in technology updates, compliance requirements, and new capabilities. A provider's financial health directly impacts their ability to support your long-term needs and maintain market competitiveness.

### What to look for in a PaaS provider

- The provider shows consistent year-over-year revenue growth in payment services, demonstrating market validation and business health
- Recurring revenue represents the clear majority of the provider's revenue, the higher the better
- R&D headcount is at or above industry benchmarks or SaaS companies, showing commitment to innovation and platform enhancement
- The provider maintains a diverse revenue base with no single customer representing concentration risk
- Professional services revenue is a small percentage of total revenue, indicating a scalable platform-based business model rather than consulting-heavy approach

### Questions on financial position

1. What percentage of your global revenue is derived specifically from banking clients? How has that changed over the past few years? Please explain.
2. What percentage of your global revenue is associated with your payments platform? What percentage is associated with other software solutions and product lines?
3. What percentage of R&D budget / headcount is focused exclusively on payments and, more importantly, your PaaS platform?
4. What percentage of your revenue comes from professional services?
5. What has been your year-over-year growth rate in the payment solutions sector? Please explain any significant variations.





## Market position

### Why this is important

As banks face growing pressure to modernize payment capabilities while managing costs, they need partners who demonstrate both established market presence and innovation ability. A provider's competitive positioning influences not just their current capabilities, but their ability to continue investing in new technologies and maintaining market-leading solutions.

### What to look for in a PaaS provider

- Proven market share in peer banks tiers / regions with demonstrated growth over the past three years, showing market leadership
- Active presence in multiple markets with scalable support teams, ensuring global reach and local expertise
- Established customer relationships with multiple institutions in your region/tier, demonstrating proven delivery capability
- Clear product roadmap aligned with key market trends (real-time payments, ISO 20022, cloud adoption), showing market understanding
- Coverage and favorable positioning in multiple analyst landscape reports, e.g., Celent, Datos Insights, IDC, Omdia and others

### Questions on market position

1. Please describe your competitive positioning in the payment solutions market, including key differentiators.
2. How do you see your market position evolving over the next 2-3 years? Please elaborate on your strategy.
3. What do you consider your key competitive advantages in the following areas: technology capabilities, market presence, customer service, and innovation?
4. Please describe your approach to market expansion, including target markets and growth strategies.
5. Please provide at least two third-party analyst reports showing your positioning relative to your competitors.



## Core platform assessment

### Why this is important

The core platform's capabilities form the foundation of your payment services and directly impact your ability to meet evolving customer needs. With **86%** of mid-tier banks preferring hybrid cloud approaches, platform flexibility and deployment options are crucial considerations for maintaining competitive advantage and operational efficiency.<sup>5</sup>

### What to look for in a PaaS provider

- Cloud-native architecture built on microservices rather than monolithic design, enabling scalability and innovation
- Proven ability to scale up to millions of transactions per day with at least 99% availability, ensuring reliable operations
- Support for multiple deployment models (public cloud, private cloud, hybrid) with consistent functionality across all options
- Comprehensive API library with hundreds of REST APIs and clear documentation, facilitating easy integration
- Real-time monitoring and auto-scaling capabilities across all deployment scenarios, supporting operational efficiency

### Questions on core platform assessment

1. What is your platform's core architecture? Please provide detailed technical specifications and diagrams.
2. Does your solution have visual workflow tools for payment orchestration?
3. Does your solution include a separate business intelligence application, including reporting dashboards?
4. Please elaborate on your platform's scalability capabilities, including: transaction processing capacity, peak load handling, and geographic distribution capabilities.
5. How does your platform handle multi-entity operations? Please describe capabilities for: multi-bank support, multi-currency processing, and cross-border operations.

<sup>5</sup> Payments Modernization Opportunity: The 2024 Mid-Tier Banking Report



## Real-time payments

### Why this is important

With **59%** of mid-tier bank customers expecting increased real-time payment usage, robust real-time processing capabilities have become essential.<sup>6</sup> Industry research indicates that offering multiple options for real-time payments provides maximum flexibility and reach for banks and their customers.

### What to look for in a PaaS provider

- 24/7/365 processing capability achieving in excess of 99% availability with the scheduled compliant annual downtime, ensuring uninterrupted payment services
- Support for multiple real-time payment types in multiple countries, with 100% scheme compliance, including Request for Payment and Request for Information, maximizing payment service flexibility
- Integration framework supporting easy connectivity to one or more third-party fraud/AML/sanctions solutions, to ensure best of breed deployment
- Monitoring system delivering real-time alerts enabling immediately response to operational issues and maintaining service quality
- Self-service capabilities for banks to build and deploy value-added real-time/instant payment services

### Questions on real-time payments

1. Please detail your real-time payment processing capabilities. How do you support 24x7 always-on operation?
2. How many different schemes do you support and in which countries? Please list.
3. Describe your approach to performance metrics, monitoring and reporting, and other operational measures of real-time payment processing health.
4. How do you handle instant payment scheme compliance across different regions?
5. Please explain your approach to real-time payment risk management.
6. How you handle smart/automating routing between different real-time networks, or between real-time and non-real-time payment schemes?
7. How do you support the bank's need to self-service in the configuration and deployment of new value-added services?

<sup>6</sup> Payments Modernization Opportunity: The 2024 Mid-Tier Banking Report



## RTGS and high-value payments

### Why this is important

High-value payment processing requires exceptional reliability and sophisticated liquidity management capabilities.

As the backbone of the financial system, these payments demand robust processing controls, comprehensive monitoring capabilities, and adherence to strict settlement windows to manage systemic risk.

### What to look for in a PaaS provider

- Support for multiple systems with annual certification and direct connectivity, ensuring reliable high-value payment processing
- Real-time liquidity monitoring managing multiple configurable thresholds with real-time alerts, optimizing liquidity utilization
- Queue management system handling multiple priority levels with automatic resolution rate, maximizing payment flow efficiency
- Payment screening completing compliance checks, ensuring secure high-value transfers
- Contingency system achieving failover with zero message loss, maintaining critical payment operations
- Processing capacity to scale up to 2x average daily volume, delivering enterprise-grade resilience for peak processing times

### Questions on RTGS and high-value payments

1. Please detail your RTGS processing capabilities across different markets.
2. How does your solution manage liquidity for high-value payments?
3. Please describe your approach to payment prioritization and queue management.
4. What controls and risk measures are in place for high-value payments?





## Low-value and bulk payments

### Why this is important

Efficient handling of bulk and low-value payments remains crucial for most banks, representing significant transaction volumes and requiring sophisticated automation. These payments demand robust file processing capabilities and efficient exception handling to maintain cost-effective operations while meeting customer service levels.

### What to look for in a PaaS provider

- Support for multiple bulk payment formats with straight-through processing, minimizing manual intervention in file processing
- Processing engine handling large volumes per file with at least 99% straight-through rate, ensuring reliable high-volume operations
- Scheduling system supporting concurrent processing windows with priority routing, optimizing payment flow management
- Reconciliation engine resolving exceptions automatically within SLAs, reducing operational overhead
- Real-time monitoring and notifications providing rapid-response file processing status updates with detailed analytics, enabling proactive issue resolution

### Questions on low-value and bulk payments:

1. Please describe your bulk payment processing capabilities and architecture.
2. How do you optimize processing for different payment types?
3. What are your batch processing capabilities and schedules?
4. Please explain your approach to payment file validation and error handling.



## Cross-border and SWIFT processing

### Why this is important

Cross-border payment capabilities are increasingly important as businesses expand globally. Recent research shows improved cross-border payments are a top priority for **52%** of mid-tier bank customers, making these capabilities essential for serving internationally active clients.<sup>7</sup>

### What to look for in a PaaS provider

- SWIFT messaging support for multiple message types with ISO 20022 compliance, ensuring comprehensive international payment capabilities
- Direct connectivity to multiple international networks with annual certification, maximizing global payment reach
- Automated FX processing handling multiple currency pairs with real-time rate updates, optimizing cross-border payment efficiency
- Compliance screening completing sanctions checks within seconds with high accuracy, reducing cross-border payment risk
- SWIFT gpi tracking providing payment status updates within agreed SLAs with automated case management, improving payment transparency

### Questions on low-value and bulk payments:

1. Please detail your SWIFT integration capabilities, including: supported message types, implementation approach, and value-added services.
2. How do you handle SWIFT gpi requirements and tracking?
3. In addition to SWIFT, how many other crossborder payment services (e.g., Visa Direct, Mastercard Send, Ripple and others) do you support? Please list.
4. How do you manage foreign exchange and currency conversion?
5. Please explain your approach to international payment compliance and screening.

<sup>7</sup> Payments Modernization Opportunity: The 2024 Mid-Tier Banking Report



## Payment schemes and rails

### Why this is important

Comprehensive support for payment schemes and rails is fundamental to a modern payment platform. Your provider must demonstrate both technical connectivity and deep understanding of scheme rules and requirements to ensure reliable operations and compliance across all payment types.

### What to look for in a PaaS provider

- Direct connectivity to minimum 5 major payment schemes with annual recertification, ensuring comprehensive market coverage and compliance
- Automated scheme updates implemented rapidly and within compliance SLAs, minimizing operational disruption during changes
- Validation engine supporting all scheme-specific rules with the ability for the bank to easily configure and deploy requirement changes, maintaining continuous compliance
- Message format processing handling at least 50+ scheme-specific protocols, ensuring reliable payment processing
- Real-time monitoring system detecting scheme issues within seconds using automated alerts, enabling proactive operational control
- Ability to intelligently route between different payment schemes based on configured rules and parameters, and/or machine learning

### Questions on payment schemes and rails

1. Please provide a comprehensive list of supported payment schemes and rails by region.
2. How do you maintain scheme compliance and manage updates?
3. Please describe your approach to new scheme integration and certification.
4. How do you handle scheme-specific requirements and rules?
5. Please explain your intelligent routing capabilities across different payment rails.



## ISO 20022 migration and standards

### Why this is important

Research indicates **62%** of mid-tier bank customers are either already using or planning to use ISO 20022 messaging formats.<sup>8</sup> This widespread adoption, coupled with major market infrastructure migrations like Fedwire®, makes robust ISO 20022 capabilities essential for maintaining competitive advantage.

### What to look for in a PaaS provider

- ISO 20022 support for multiple domestic ISO 20022 based schemes, demonstrating comprehensive implementation expertise
- Automated message transformation processing MT/MX conversions daily with 100% accuracy, ensuring reliable format coexistence
- Built-in validation engine supporting 20+ scheme specific ISO variations with regular rule updates, maintaining continuous scheme compliance
- Version management system handling 2+ concurrent ISO versions with zero-downtime updates, simplifying standards evolution
- Extended ISO 20022 data processing capturing all necessary fields for analytics and reporting, maximizing value from rich payment data

### Questions on ISO 20022 migration and standards

1. Please detail your ISO 20022 implementation approach and capabilities.
2. How do you handle coexistence of MT and MX messages?
3. Please describe your ISO 20022 migration support services.
4. What tools do you provide for message validation and transformation?
5. How do you manage version updates and maintenance of message standards?
6. What, in your view, are the top factors contributing to the success of an ISO 20022 migration, for either domestic or cross-border payments?
7. How do you enable customers to take advantage of the extended data envelope in ISO 20022, beyond basic compliance?

<sup>8</sup> Payments Modernization Opportunity: The 2024 Mid-Tier Banking Report





## Architecture and deployment

### Why this is important

Cloud adoption is accelerating in payments, with Volante's research showing **76%** of mid-tier banks plan significant investments in commercial payments technology.<sup>9</sup> Your provider's architectural foundation and deployment flexibility directly impacts your ability to scale, innovate, and manage costs effectively.

### What to look for in a PaaS provider

- Cloud-native architecture processing scalable to millions of daily transactions with at least 99% availability, ensuring dependable scalability across all deployment types
- Ability to deploy on different clouds (AWS, Azure, GCP, etc.) in a cloud-agnostic manner, providing deployment flexibility and vendor independence
- Automated deployment system achieving zero-downtime upgrades within 30-minute windows, minimizing operational disruption
- Disaster recovery system maintaining RTO under 2 hours and RPO under 15 minutes, guaranteeing business continuity for critical functions
- Security controls certified against NIST and ISO standards across all deployment models, ensuring consistent protection regardless of architecture

### Questions on architecture and deployment

1. Please describe in detail your cloud deployment strategy, including: public vs. private cloud approaches, hybrid deployment options, and security considerations.
2. What pre-built integrations do you offer for: core banking systems, treasury systems, risk management platforms, and other key banking systems?
3. Please explain your approach to scalability and performance optimization.
4. How do you handle disaster recovery and business continuity?

<sup>9</sup> Payments Modernization Opportunity: The 2024 Mid-Tier Banking Report



## Integration capabilities

### Why this is important

In today's interconnected banking environment, integration flexibility is crucial for success. With banks increasingly focused on modernization and automation, your provider's integration capabilities directly impact your ability to deliver seamless services across your technology ecosystem.

### What to look for in a PaaS provider

- Pre-built integrations with major core banking systems and treasury platforms, accelerating implementation and reducing custom development costs
- API library containing relevant documentation with dedicated sandbox environments, enabling rapid development and testing of custom integrations
- Support for processing thousands of real-time and several hundred batch transactions daily, ensuring scalability across all integration patterns
- Built-in transformation engine supporting 50+ industry message formats with high-accuracy, streamlining cross-system communication
- Automated testing suite covering of integration scenarios with deployment validation under 1 hour, minimizing integration risk
- Low-code/no-code capabilities allowing for rapid configuration of integration endpoints without requiring development resources or upgrades/customization

### Questions on integration capabilities

1. Please detail your integration architecture and supported methods.
2. What pre-built integrations do you offer for: core banking systems, treasury systems, risk management platforms, and other key banking systems?
3. Please describe your API strategy and capabilities.
4. How do you support custom integration development?
5. What is your typical integration timeline for different scenarios?



## Configurability and self-service

### Why this is important

In today's rapidly evolving payments landscape, banks need efficient ways to adapt platform capabilities to their specific needs. The ability to configure and manage platform settings and manage message transformation without vendor intervention enables faster response to market changes and reduces operational overhead.

### What to look for in a PaaS provider

- Visual workflow tools supporting predefined payment flows without coding, enabling rapid service deployment without technical expertise
- Visual mapping and enrichment of messages moving from one message type to another, ensuring ease in supporting multiple message types across all internal systems
- Self-service dashboard, empowering business users to manage payment operations independently
- Library of pre-built payment templates customizable within minutes, accelerating adaptation to new business requirements
- Report builder interface with access to 100+ payment data fields and automated scheduling, enabling business users to gain operational insights without IT support

### Questions on configurability and self-service

1. Please describe your development environment and tools.
2. Does your solution support the ability to make workflow orchestration changes using visual or low-code components? If so, how?
3. How do you support client-specific customizations?
4. Please explain your approach to version control and release management.
5. How do you handle custom development requests?



## Security architecture

### Why this is important

Payment security requirements continue to evolve rapidly, with sophisticated threats demanding equally sophisticated defenses. As banks handle increasingly complex payment flows, robust security architecture becomes fundamental to maintaining customer trust and regulatory compliance.

### What to look for in a PaaS provider

- Annual renewal of PCI-DSS Level 1, ISO 27001, and SOC 2 Type 2 with zero major findings, demonstrating rigorous adherence to global security standards
- 256-bit end-to-end encryption with multiple distinct security layers, ensuring comprehensive protection against sophisticated cyber threats
- Real-time threat monitoring with maximum 5-minute detection-to-response time, minimizing impact of security incidents
- Role-based access control with minimum 5 hierarchical permission levels for granular activity control, ensuring precise system access management
- Automated audit logging with 7-year retention and sub-second search capabilities, supporting regulatory compliance and rapid forensic analysis

### Questions on security architecture:

1. Please provide a detailed overview of your security architecture, including diagrams where available.
2. How do you implement multi-layered security controls? Explain why you took this approach.
3. Please describe your approach to: access control, data encryption, key management, and audit logging.
4. What security certifications do you maintain? Please distinguish between those provided inherently by the cloud provider you are using to provide your service and those which are held by your organization.



Review our bonus security checklist, which highlights the importance of choosing a PaaS provider with a track record you can trust.



# PaaS vendor security checklist

As organizations adopt cloud-based payment solutions, choosing a Payments as a Service (PaaS) provider with strong security measures and, most importantly, a proven history of zero security breaches is more crucial than ever. Financial institutions are increasingly prioritizing data security and breach prevention in response to evolving cyber threats.<sup>1</sup>



**49%**

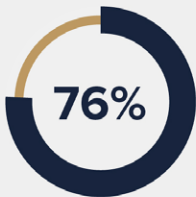
of attacks against financial institutions originated from phishing



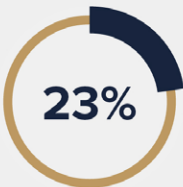
**20%**

of ransomware attacks in the sector were against banking institutions

Fraudsters have shifted away from digital payments fraud to social engineering tactics that exploit the trust of their victims. Due to this risk...



of Financial Institutions are either in the process of adding new technologies or planning to do so in the next year.<sup>2</sup>



of all fraudulent transactions are from scams, the most common form of fraud reported by banks. This is a 56% increase in the share of fraudulent transactions that are scams from the previous year.<sup>2</sup>



of FIs have implemented behavioral analytics technology in the last year. FIs are turning to newer anti-fraud technologies that support them in identifying social engineering strategies.<sup>2</sup>

<sup>1</sup> 2024 Trustwave Risk Radar Report: Financial Services

<sup>2</sup> PYMNTS: The State of Fraud and Financial Crime in the U.S. 2024: What FIs Need to Know

Achieve a competitive edge by ensuring your Payments as a Service provider is equipped to combat cyber threats while complementing your bank-level security offerings:

Features	Capabilities
Security against unauthorized access	<ul style="list-style-type: none"> <li>✓ Enforcing a strong password policy</li> <li>✓ Applying 2-Factor Authentication</li> <li>✓ Sending login data over a secure channel – HTTPs, SFTP and Teleport required</li> <li>✓ Single Sign On (SSO) with Multi-Factor Authorization (MFA) required for privileged data access</li> <li>✓ Email mailboxes are encrypted and have advanced malware and phishing detection</li> <li>✓ Enforcing separation of duties with role-based access that lets you control who can enter, approve, and pay Volante Payments Platform automatically keeps record and audit trail of all payment transactions, including associated payment details.</li> <li>✓ Information security team reviews ownership of user accounts and access management</li> </ul>
Risk and Compliance	<ul style="list-style-type: none"> <li>✓ Undergo an annual SOC 1 and SOC 2 Type 2 Audit by a leading international CPA Firm</li> <li>✓ Employees undergo background checks and data security and privacy training</li> <li>✓ Vulnerability Assessment and Penetration Testing (VAPT) are conducted annually on platform systems to identify or address potential cyber security vulnerabilities</li> <li>✓ Integrates with partner or bank's Anti-Money Laundering (AML)/Office of Foreign Assets Control (OFAC) Program, which is designed to prevent money laundering, terrorist financing, violating or subverting OFAC sanctions, or for other illegal purposes</li> <li>✓ Integrates with partner or bank's Know Your Customer ("KYC") practice to ensure accuracy and legitimacy of payment accounts</li> <li>✓ Integrates with partner or bank's Account Validation Services (AVS) to verify the authenticity of payment information and mitigate fraud risks.</li> </ul>
Network Security	<ul style="list-style-type: none"> <li>✓ Uses IPS IDS and web application firewalls (WAF) for intrusion detection, prevention of unauthorized electronic access to our servers</li> </ul>
Data Security	<ul style="list-style-type: none"> <li>✓ Uses NOC/SOC Network &amp; Security Event Monitoring &amp; Response systems for 24/7 monitoring, incident response, and incident management</li> <li>✓ Data in transit is encrypted over secure channel</li> <li>✓ Maintains continuity and regulatory backups that are encrypted using industry standard AES-256</li> <li>✓ Tests its Business Continuity Plan (BCP) or Disaster Recovery Plan annually to ensure rapid recovery to be proactive against any possible service disruption</li> <li>✓ Antivirus software running in background of devices, e.g., employee computers</li> <li>✓ Secure configurations for servers, data bases and other production components</li> </ul>
Security Certifications that cover application, data, infrastructure and privacy	<ul style="list-style-type: none"> <li>✓ PCI DSS 4.0 - Data Security</li> <li>✓ SOC 1 Type 2 and SOC 2 Type 2</li> <li>✓ ISO 27001 – ISMS</li> <li>✓ ISO 27017 – for the Cloud Security</li> <li>✓ ISO 27018 – Privacy extension for Cloud</li> <li>✓ ISO 27701 – Privacy Information Management System</li> </ul>
Secure payment rail connections	<ul style="list-style-type: none"> <li>✓ Offers banks and financial institutions secure connection to ACH, Wires, TCH RTP, SEPA and cross-border payments</li> </ul>



## Regulatory compliance

### Why this is important

In today's complex payments landscape, compliance requirements vary significantly across jurisdictions and consume an increasing portion of technology budgets. Your provider's compliance capabilities and architecture directly impact your ability to manage regulatory risk efficiently while maintaining competitive service levels. An open architecture approach enables you to leverage best-of-breed compliance solutions while ensuring consistent regulatory coverage across all payment types.

### What to look for in a PaaS provider

- Open architecture supporting integration with multiple compliance providers (AML, sanctions, fraud), enabling best-of-breed solution adoption while maintaining operational efficiency
- Support for real-time compliance screening across all payment types with sub-second processing times ensuring minimal impact on payment processing
- Automated regulatory change management system that implements updates across all jurisdictions within 30 days of announcement, maintaining continuous compliance
- Comprehensive audit trails with minimum 7-year retention and searchable access to all compliance-related activities, supporting regulatory examinations
- Pre-built regulatory reporting templates covering major global jurisdictions with automated data collection and validation, reducing manual effort and error risk
- Integration with at least 3 major global compliance data providers (e.g., sanctions lists, PEP databases), ensuring comprehensive screening coverage

### Questions on regulatory compliance

1. How do you ensure compliance with banking regulations across different jurisdictions?
2. Please describe your approach to integrating with AML screening, sanctions checking, fraud detection, and transaction monitoring solutions.
3. How do you stay current with regulatory changes? Please describe your process and approach in detail.
4. What compliance reporting capabilities do you offer? Are those reports made available to clients? If so, how often can clients request them and what is the expected delivery timeframe.



## Product roadmap

### Why this is important

A provider's product development strategy and execution capabilities directly impact your ability to stay competitive. With mid-tier banks facing increasing pressure to enhance real-time processing, data access, and automation capabilities, your provider's roadmap and proven ability to deliver against it will significantly influence your success.

### What to look for in a PaaS provider

- Documented track record of delivering key roadmap features within committed timeframes over the past 24 months, demonstrating reliable execution
- Roadmap reviews with client advisory board participation, ensuring customer needs directly influence development priorities
- Clear alignment between roadmap priorities and major industry initiatives (e.g., ISO 20022, real-time payments, cloud adoption), showing market understanding
- Transparent development methodology with regular progress updates and early access programs for major features, enabling clients to plan effectively
- Roadmap items directly sourced from client feedback and enhancement requests, proving responsiveness to customer needs

### Questions on product roadmap:

1. Please provide a product roadmap for the next 24 months. Include strategic themes driving your roadmap.
2. How do you prioritize new feature development?
3. Please describe your approach to incorporating emerging technologies.
4. How do you involve clients in product development decisions?
5. What major innovations are you planning in the following four areas: payment processing, client experience, operational efficiency, and risk management?
6. Please discuss your performance against road mapped features and timelines over the past 2 years.





## Onboarding, training, and support

### Why this is important

As payment systems grow more complex, your provider's ability to deliver efficient onboarding, comprehensive training, and responsive support directly impacts your operational success and risk management. The right combination of standardized methodology and flexible support ensures smooth transition and reliable ongoing operations while maintaining high service levels.

### What to look for in a PaaS provider

- Proven onboarding methodology with 180-days or less standard implementation timeframes for standard product deployments, demonstrating efficient delivery capabilities
- 24/7 support coverage with quick response times for critical incidents and SLA adherence, ensuring reliable operations
- Comprehensive training program covering technical, operational, and business user roles with both self-paced and instructor-led options, enabling effective knowledge transfer
- Dedicated client success team with quarterly service reviews and proactive optimization recommendations, supporting continuous improvement
- Self-service portal with extensive documentation, video tutorials, and sandbox environments, empowering clients to resolve issues independently

### Questions on onboarding, training, and support:

1. Please describe your standard onboarding methodology.
2. What is your typical onboarding timeline for different scenarios?
3. How do you handle data migration and legacy system integration?
4. Please describe your client success program.
5. Please detail your support model and service levels.
6. What training programs do you offer? Please describe delivery methods and content.
7. How do you handle: system updates, emergency support, change requests, and performance optimization?
8. Please describe your client success program.



## Pricing structure

### Why this is important

Understanding total cost of ownership is fundamental to making informed payment platform decisions. Your provider's pricing structure impacts not only initial implementation costs but long-term operational expenses, making transparency and predictability essential for accurate budgeting and growth planning. The right pricing model should scale efficiently with your business while providing clear visibility into all cost components.

### What to look for in a PaaS provider

- Transparent subscription-based pricing with all costs documented upfront and no hidden fees, enabling accurate budget planning
- Volume-based pricing options based on tiers, rewarding growth with lower per-transaction costs
- Predictable monthly costs combining base platform fee with transaction-based pricing, preventing unexpected expense variations
- Clear cost allocation across different payment types and value-added services, allowing precise ROI calculations
- Flexible pricing options allowing you to align service cost with your bank's business and revenue goals

### Questions on pricing structure:

1. Please provide a detailed breakdown of your pricing model, including: license fees, implementation costs, support and maintenance fees, and transaction-based pricing.
2. Please discuss your pricing structure for different deployment models, various payment types, and value-added services.
3. What factors influence pricing variations? What is the magnitude of those variations?
4. Please describe any volume-based discounting options.

## Conclusion: Moving forward with PaaS provider selection

Selecting a Payments as a Service (PaaS) provider will shape your institution's success or failure. While technical functionality forms the foundation of any PaaS solution, success depends on looking beyond surface capabilities to evaluate organizational stability, market position, and long-term viability. The provider's security framework, compliance capabilities, and implementation approach are equally crucial as they significantly impact both your transition experience and ongoing operations.

The payments landscape continues to evolve, with new technologies, schemes, and customer expectations emerging regularly. Your success depends on selecting a provider who can demonstrate not just current capabilities but the vision, resources, and commitment to help you navigate the changing market.

### Six recommendations for a successful selection experience:

- 1** Prioritize providers with proven financial stability and a clear commitment to payments innovation, demonstrated through consistent R&D investment and market presence
- 2** Ensure comprehensive security and compliance frameworks that can adapt to evolving regulatory requirements across your operating jurisdictions
- 3** Look for flexible deployment options, particularly hybrid cloud capabilities, to support your specific operational needs and future scaling requirements
- 4** Validate the provider's implementation methodology and support model through reference checks and detailed evaluation of their client success programs
- 5** Evaluate the provider's real-time payment capabilities and ISO 20022 readiness as these are fundamental requirements for future growth
- 6** Avoid over-customization of vendor products to match legacy requirements, and favor providers that can meet your requirements through configuration



## About Volante Technologies

Volante Technologies is the trusted cloud payments modernization partner to financial businesses worldwide, giving them the freedom to evolve and innovate at record speed. Real-time native, API enabled, and ISO 20022 fluent, Volante's Payments as a Service and underlying low-code platform process millions of mission-critical transactions and trillions in value daily. Volante's customers include four of the top five global corporate banks, seven of the top ten U.S. banks, and two of the world's largest card networks.

LEARN MORE



[www.volantetech.com](https://www.volantetech.com)



[/volante-technologies](https://www.linkedin.com/company/volante-technologies)



[/volantetech](https://twitter.com/volantetech)