

FinTech Self-Assessment Checklist for Financial Institution Partnerships

Introduction:

As partnerships between FinTechs and traditional financial institutions play an increasingly important role in driving innovation and compliance, it is important for FinTechs to ensure they meet key regulatory, operational, and strategic requirements.

This self-assessment checklist is designed to help FinTechs evaluate their readiness to engage and collaborate with banks and other financial institutions. It offers a structured approach to identifying areas of strength, addressing potential gaps, and preparing for effective partnerships.

By using this tool, FinTechs can better understand their alignment with industry standards and position themselves for integration into the broader financial ecosystem.



Question	Yes	No
Company Profile		
Do you have a company size of at least 20 employees?		
Has your company been in operation for at least 3 years?		
Do you have measures to mitigate against keyman risk?		
Do you have a presence in Singapore?		
Does your founder have at least 10 years of relevant experience in the financial services or technology sector?		
Business Model and Value Proposition		
Are you clear about your target beneficiaries/users?		
Are you able to articulate the problem statement/use cases that your solution/product addresses?		
Are you able to articulate the unique selling proposition of your solution/product?		
Can your solution scale to meet the demands of large financial institutions?		
Is your costing model competitive compared to market rates?		
Do you have at least 1 bank/ FI/ large company as a client?		
Is your solution scalable in at least 2 countries, taking into consideration local regulations and data requirements in other countries?		
Regulatory Compliance		
Do you have a compliance team?		
Are you compliant with all of the following financial regulations or guidelines (if applicable)? <ul style="list-style-type: none"> • Anti-Money Laundering (AML)/ Counter-Terrorism Financing (CFT) • Know Your Customer (KYC) • Personal Data Protection Act (PDPA) 		
Have you obtained the following licenses, registrations or certifications (if applicable)? <ul style="list-style-type: none"> • Outsourced Service Provider Audit Report (OSPAR) • ISO 27001 • ISO 20022 • PSD2 • PCI DSS 		
Do you have a data retention policy that is compliant with local regulations?		
Do you have zero data breach cases in the last 2 years?		
Do you have zero AML breach cases in the last 3 years?		
Do you have zero adverse news or on-going litigation?		
Security and Risk Management		
Are you familiar with the Technology Risk Management (TRM) guidelines?		
Is your data securely backed up with incorporated redundancies?		
Do you have a comprehensive cybersecurity strategy, including regular vulnerability assessments and penetration testing?		

Does your solution have high security standards with features such as encryption/ multi-factor authentication and regular security audits?		
Have you implemented strong encryption methods for sensitive data at rest and in transit, adhering to industry standards and regulations?		
Do you support standard login options such as OAuth 2.0, OpenID Connect, SAML?		
In terms of user ID management, do you support single sign-on and/or dedicated ID?		
Do you regularly conduct incident response and disaster recovery simulations?		
Do you have measures to mitigate the risks that your solution/product poses to your clients?		
Are all components of your solution/ product reviewed on a regular basis and monitored in real-time?		
Financial Stability		
Do you have a runway of at least 18 months of funding and assets/capital to sustain operations?		
Are you at post-revenue stage?		
Do you have a strong cap table or strategic/reputable investor(s)?		
Are your financial statements regularly audited and up to date?		
Technology Infrastructure		
Do you offer multiple connectivity options for easy integration with existing systems e.g., APIs?		
Is your solution deployment mode agnostic?		
Are you able to support multi-country implementation with logical segregation within the application?		
Is your system architecture cloud native (i.e., micro-service based, event driven, API-enabled and running on containers)?		
Do you have no or minimal dependencies on third party service providers?		
Do you use open-source technologies?		
For SaaS providers, do you use more than 1 cloud service provider?		
Can your solution provide real-time data and analytics in useful formats (e.g., Power BI dashboard) for informed decision making (if applicable)?		
Customer Support and Experience		
Have you mapped your user journeys to ensure a user-friendly interface for users at every stage?		
Are you able to provide technical support within 24 hours?		
Do you have a local technical support team?		
Can you provide 24/7 customer support if required?		