Uncovering value in embedded finance for Banking & Capital Markets

Managing risks in the transition to integrated financial services

July 2023

The competitive landscape of embedded finance is evolving. Players must expand their risk awareness to grow and remain resilient.

Embedded finance presents a compelling set of possibilities for businesses to reach customers in new ways, build operational scale, and rethink how products and services are deployed. By offering financial services, platforms can deepen their relationship with customers and provide them with additional value beyond their core products. As is often the case with new opportunities, there are risks to consider.

As we have written about previously, success across the challenging assumptions to chart new growth — requires a major shift in mindset and capabilities. Our proprietary risk framework sets out five emerging areas for participants within financial ecosystems to consider, stretching beyond existing risks that are inherent to financial products. The five areas include interoperability, data containment, complex partnerships, vulnerable customers, and distributed risks. Forming an understanding of each of these is critical to managing emerging risks in a prudent and collaborative manner.

The embedded finance risk framework

We have identified five elements that consistently influence the embedded finance journey: compatibility, data containment, complex partnerships, vulnerable customers and distributed risk. New areas of focus within these topics point to important risk implications for all players, but particularly for incumbent banks, who must double down on specific priorities: tech-powered transformation, data-enabled customer focus and an entrepreneurial approach to relationship-building.

The five elements of the embedded finance risk framework

Risk element	Implications
Compatibility	Risks associated with the connection and communication between fundamental components that enable embedded finance: technology such as APIs, microservices and private cloud, and operational resilience, such as incident response and disaster recovery
Data containment	Data security, privacy, and control issues regarding fractional data use and ownership, which is often at odds with consumer and client expectations of seamlessness in their interactions and transactions
Complex partnerships	Risks stemming from the unique nature and complexity of embedded finance partnerships, such as one-to-many, shared liability, and third-, fourth- and fifth-party relationships among providers, vendors and financial institutions
Vulnerable customers	Customer-specific concerns arising from partnerships between financially regulated and non-regulated institutions, including: increased use of data harvesting, profiling and monetisation, duty of care, marketing, cross-selling, and customer retention and loyalty
Distributed risk	The exponential increase in risk transfer within complex embedded finance ecosystems—reinforcing the need to develop an effective risk management approach for distributed risk and shifting liabilities

Compatibility

Embedded finance depends on compatibility, which refers to the ability of different parties and systems to work together seamlessly. This involves having the right cloud architecture, authentication services, and embedded finance API technology to facilitate transactions between organisations. However, managing the multiple intermediary partners involved in embedded finance ecosystems requires careful consideration of accountability and risks related to component compatibility between technologies, customer user experience (UX), and ecosystem partners. To do this, companies must develop new tech capabilities and a robust strategy to address these challenges and ensure open, cloud-based architecture.

Geopolitical considerations, such as restrictions on foreign cloud service providers and media platforms, can complicate the development of an effective embedded finance strategy. Banks often build cloud data centers in different regions based on diverse regional regulations. Similarly, in the payment industry, the availability and compatibility of point-of-sale service offerings can vary depending on the system integrator or technology vendor in a specific region. This highlights the importance of a robust compatibility strategy that takes into account these factors and enables companies to navigate the challenges effectively. Ultimately, banking institutions need to update their technology stack and take steps towards open-ended architecture by building up their digital capabilities and talent, whilst enhancing their risk management. New entrants that demonstrate a credible risk management function, tailored to handle unique and emerging operational and compliance risks, will be winners within competitive markets.

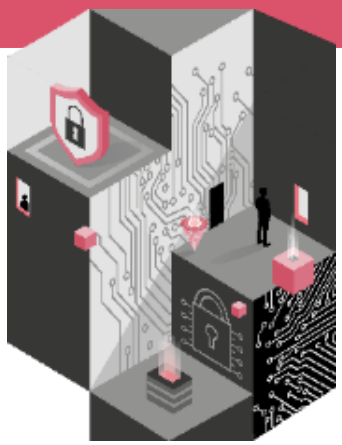
A fully articulated compatibility strategy can reduce costs and unlock enhanced revenue and new business opportunities. Open architecture enables banks to develop technological capabilities and innovative financial solutions that are compatible and customisable across platforms. Recognising banks as software- and technology-enabling partners expands the scope of services they can provide to customer-facing platforms, including integrating existing products and services into embedded finance ecosystems.

Data containment

Data allows companies to retain customer loyalty in specific ecosystems and underpins the provision of seamless customer experiences. In embedded finance, customer data is typically exchanged by multiple players, from the formulation of privacy and data sharing agreements, to obtaining consent for data capture and sharing. In this ecosystem, sharing customer data among financial organisations, digital platforms and product-led fintech creates new vulnerabilities. Larger banks and other incumbent financial institutions, which have built reputations as stewards of customer data, now need to do more through collective and coordinated efforts to maintain customer confidence, trust, and loyalty. However, the complexities of open architectures lead to an increase in the partial ownership and usage of data, these broader questions pose significant risks, alongside security concerns such as data theft, breaches and cyberattacks.

Data privacy regulations and security from consumer watchdog agencies will increase pressure on risk functions. Customers are at risk from both intentionally misused data and unintentional, improper data handling. In 2021, Data Security Law and the Personal Information Protection Law have started to be strictly enforced in China. To counter these data containment risks and ensure strong controls on data security, privacy, and consumer protection, organisations in embedded finance networks require more sophisticated data governance and technology risk management programmes than are currently in place. There have been reports of data breaches and other cybersecurity incidents connected to tech companies involving in embedded finance in China. One of the biggest Chinese ride-hailing firm was fined in 2022 for over eight billion yuan for breaking the data security laws. Therefore, data security is really a big concern for Chinese government and companies must enhance their system constantly to avoid any potential data risk.

Organisations will also need to be attuned to emerging risks from new models and algorithms that consume and transform alternative data. These can lead to challenges such as data (and data analytics) being used in ways that are unfair, discriminatory or non-transparent to both consumers and regulators.



Complex partnerships

In embedded finance, partnership risk could be broad, owing to the complexities of open architecture, new monetisation strategies and the need to shift from a liabilities management mindset to a more collaborative approach.

Consider a scenario where a bank offers its services to customers through white labelling in collaboration with a non-banking institution. This could be beneficial for both parties, as non-banking institution leverages bank's ability to offer regulated financial services to better serve their customers, while the bank can expand its customer base and gain a role in a new business channel. Nevertheless, it is equally important for banks to consider their role in the embedded finance ecosystem. As the landscape of embedded finance continues to evolve, banks may not derive significant benefits from providing white label banking services, especially if the non-banking institutions are primarily responsible for customer acquisition and retention.

Another example is the two-way partnership that needs to exist between fintech companies and a sponsor organisation, such as a big bank or insurer. It is necessary for the bank to understand how fintech companies manage risks and obligations in an effective manner, without just transferring the underlying risks back to them. At the same time, fintech companies need access to the bank's technology stack, and they must also understand how any supporting services are being performed, such as credit underwriting, KYC and transaction monitoring.

However, these partnerships can create complex relationships that may be challenging to manage. Disagreements may arise over revenue sharing, data sharing, and liability in the event of fraud or financial crime. This is particularly evident in partnerships between Chinese tech giants like Alibaba or Tencent and multiple financial institutions, which can further complicate relationships and increase the risk of conflict of interest.

When approaching these partnerships strategically, companies not only diversify their risk exposure but create a resilient business process and IT ecosystem that allows them to be agile. With the right partnerships, companies can break into new embedded finance markets, building innovative products and services within the ever-changing fintech environment.

Vulnerable customers

With the application of embedded finance, non-banking organisations in virtually any industry can break into financial services without taking on the significant regulatory burden associated with the sector. This creates a unique risk around customer ownership for all parties, and particularly for incumbent financial organisations. The importance of properly assessing vulnerable customer risk is highlighted in a dispute involving Australian buy-now-pay-later (BNPL) providers that failed to adequately assess customers' creditworthiness and affordability, leading to customers taking on unsustainable debt in 2021.

Each party in this ecosystem is confused about its own responsibility in the process: Who owns which piece of the customer relationship? Does the bank own the right to cross-sell to that customer for lending and other credit opportunities? Who is responsible for the duty of care of customers who are being incentivised to spend—and could do so beyond their means?

To avoid this risk, organisations which offering embedded finance must ensure their products and services considers customer ownership pre-emptively — giving partners sufficient rights to the customer relationship. Additionally, organisations must manage the risks associated with how they, and their partners, communicate with customers and generate brand loyalty to their products and services.

Distributed risk

Distributed risk — the increase in risk transfer across complex ecosystems—is the culmination of all the risks we have outlined up to this point. This type of risk, which is shared among many players, has existed within financial relationships for decades, an example being how a bank may white label its services through a credit card provider and a payment processor. However, the risk has become exponentially greater within embedded ecosystems that involve more players touching the same data and transactions, often at the same time.

Regulated banks and financial institutions, which are accountable and liable for securing customer data as it passes through the multiplayer distributed ecosystem, therefore take on additional data protection responsibilities with open-banking relationships. In cases where financial institutions engage or partner with third-party service providers, such as e-commerce platforms, to launch BNPL products, financial institutions will be responsible and accountable for the actions of those third-party service providers from the customers' perspective. As a result, proper mechanisms and controls are expected to be put in place to manage potential issues, such as consumer protection issues. In 2022, the HKMA enforced the enhancing consumer protection in respect of BNPL products, and other relevant guidance has been issued by the HKMA to improve the regulatory system.

Lack of awareness and knowledge around security and risk management practices of their third-, fourth- and fifth-party vendors can quickly spiral out of hand. For instance, peer-to-peer (P2P) lending platform business was flourishing in mainland China before 2018, allowing individual investors to lend money directly to individual borrowers with the platform acting as an intermediary. The risk of credit and fraud were distributed across the platform, the underwriting financial institutions, and the individual investors. However, as the industry grew rapidly, so did the number of fraudulent and failed P2P platforms. The mainland Chinese government began cracking down on the industry, with over 5,000 platforms shutting down by the end of 2019, leaving investors with billions of dollars in losses.
This example highlights the importance of managing distributed risks in embedded finance and the need for effective oversight and regulation to protect investors and the broader financial system.

When tackling distributed risk, traditional risk management practices remain effective, but companies must bolster them with new techniques and approaches to ensure effective oversight and mitigation where appropriate. Implementing risk management frameworks and operationalising periodic third-party risk assessment programmes can help identify distributed risks among the various vendor parties. But it is crucial to consistently challenge historical organisational biases and experiences — especially as distributed risks evolve with the growing adoption of embedded finance.

Looking ahead

As the landscape of embedded finance continues to evolve, it is crucial for businesses to expand their risk awareness and adopt a proactive approach to risk management. At PwC, we offer a range of services to help banks and also non-bank businesses navigate the complexities of embedded finance.

What PwC offering:

- Embedded finance go-to-market and growth strategy
- Risk assessment and management advisory services
- Technology and data governance services
- Partnership selection and interoperability assessment
- Customer protection and vulnerability assessment
- Regulatory compliance and reporting services

To have further conversation on this topic, please contact:

Brian Yiu
Partner
brian.ky.yiu@hk.pwc.com

James Tam
Banking and Capital Markets Leader
james.tam@hk.pwc.com

Philip Chan
Partner
philip.mk.chan@hk.pwc.com

Rondy Wong
Associate Director
rondy.lh.wong@hk.pwc.com

We would also like to acknowledge the following team members who have contributed significantly to this paper: Eriko Yik, Michelle Wang