pwc

GLOBAL FINTECH FEST

Unlocking efficiency through ring-fencing in the financial services sector

October 2025

1 An overview of India's financial services sector: From analogue to digital

More than a decade ago, financial services in India were grounded in analogue routines. Insurance was typically sold door-to-door by agents who visited customers with thick brochures. Stockbrokers helped clients open physical demat accounts and executed trades over the phone. Most payments were made in cash, by cheque or with physical cards. Each activity operated in a silo and often involved manual, paperwork-heavy and slow processes.

The concept of integrated financial services began to emerge around that time. Rather than handling each product in isolation, some companies – whether as issuers or as distributors of multiple products – began bundling multiple financial offerings under a single entity or across multiple entities within a group. This development set the stage for a digital transformation that reshaped financial services business models and the broader ecosystem.

The analogue era was disrupted by a sudden wave of digitisation, strong policy support for digital infrastructure and the arrival of FinTechs as new stakeholders. Together, these factors radically transformed India's financial services landscape. The emergence of internet banking, online broking platforms, digital wallets and mobile apps removed friction from everyday financial tasks. At the same time, the development of public digital rails and continuous improvements in digital infrastructure further accelerated financial inclusion and enhanced convenience.

Today, India's financial world is no longer a simple landscape of banks, stockbrokers and insurance companies – it has become a bustling metropolis where tradition converges with disruption at every juncture.

From the customer's perspective, expectations have evolved rapidly. Users now seek integrated, end-to-end digital experiences and no longer want to visit branches for their smallest financial needs. Over time, their expectations have evolved further. They do not want to toggle between multiple apps for every financial need and prefer a single, seamless experience for all their financial needs, including payments, investments and protection.

2 Rising aspirations, declining margins

With the transformation in financial services, agility and innovation have become essential for the sustainable growth of any entity or group connected to a financial product. India's financial ecosystem includes both FinTech innovators and traditional business houses/financial conglomerates (jointly referred to as 'financial service providers' [FSPs]). These FSPs have played a pivotal role in driving growth and innovations. By broadening their capabilities, acquiring new licences, expanding distribution services and forging partnering across the value chain, they have kept pace with the rapidly changing financial landscape while continuing to deliver a rich customer experience.

Business models began evolving, with regulated and non-regulated arms/businesses of the same group operating side by side. This coexistence, which was certainly far from accidental, unlocked synergies and efficiencies over time. Once a customer was onboarded for a particular financial product, additional offerings could be cross-sold through data sharing, thereby optimising initial onboarding costs and generating incremental revenues.

This strategy of becoming a one-stop solution for all the customer's financial needs was successful initially. Over time, however, margins began to thin, owing to the following factors:

- More innovators and business groups entered the space, resulting in intense competition.
- Policymakers restricted, prohibited or capped certain revenue streams to make financial products accessible to the last-mile population.
- Regulated businesses faced growing compliance requirements as regulations evolved.

The combination of squeezed margins and restricted revenue streams has led to bottlenecks for many players. These pressures not only tested the resilience of existing models but also pushed the players to seek new ways of sustaining scale and profitability.

3 Towards cost efficiency and centralisation

With an aspiration to 'make more with less', FSPs focused on cost efficiency, leading them to explore the option of centralisation of functions and activities. Promoters also considered alternatives, such as build versus outsource or participating in the financial ecosystem as issuers or distribution partners. However, centralisation emerged in the financial ecosystem as one of the quickest means to reduce costs compared with other options that could be pursued in parallel. The logic for centralisation was simple: Why duplicate functions across multiple licensed entities when they could be pooled under a single shared structure to deliver tangible benefits?

While technology platforms, HR and payroll, customer service centres and data analytics emerged as obvious functions for centralisation, over time, the scope extended to encompass a broader range of business-related functions. This trend mirrors the evolution of global capability centres (GCCs) and shared services hubs – a model recognised globally for operational excellence.

However, centralisation introduced its own complexities, especially from the governance, risk and compliance standpoint. The conflict between the strategic goal of reducing costs through centralisation and the regulatory requirement of maintaining entity-level independence began to surface – a friction that lies at the heart of governance, particularly for regulated entities.

This raises important questions: How much centralisation is too much? At what point does efficiency begin to erode accountability?

In the next section, we explore these issues in greater detail.

4 Fault lines of centralisation

Over the years, centralisation has become both a logical choice and, in many ways, a necessity, particularly in a market environment where entry is relatively easy but sustaining competitiveness proves far more challenging. However, this approach has revealed governance complexities that warrant closer scrutiny as the clear boundaries between regulated and non-regulated businesses begin to blur. At this stage, the focus is no longer on whether firms innovate, but on whether they do so responsibly within the guardrails of regulation, accountability and customer trust. Consequently, the efficiencies achieved through centralisation must be carefully weighed against associated governance and risk considerations, which can include the following:

Dilution of entity-level accountability

Financial sector regulators such as the Reserve Bank of India, Securities and Exchange Board of India and Insurance Regulatory and Development Authority of India emphasise that accountability must rest with the licensed entity. However, in practice, decision making often shifts to group-level committees or shared functions. When boards of regulated entities defer to a centralised group authority, their independence may be compromised. In turn, this raises concerns about whether the 'mind and management' of the regulated entity truly lie within that entity – a principle embedded in regulatory frameworks across financial sectors.

Dilemma of determining core vs. non-core functions

Many regulated entities may begin to centralise functions that are core to the operations of the licensed entity. From a regulatory perspective, such arrangements may start falling within the ambit of outsourcing. While regulatory guidance clearly prescribes what can be and cannot be outsourced – with the latter being more explicitly defined in practice – application often rests on principle-based interpretation and the regulator's perception of intent. For instance, regulators have, in certain contexts, expressly restricted outsourcing critical functions, such as decision making relating to compliance with know your customer (KYC) norms. The challenge lies in the multiple layers of supporting activities that feed into these decisions. These ancillary steps, which can involve dozens of sub-functions, are not always explicitly addressed within regulatory frameworks. This creates a zone of subjectivity where entities, under the banner of centralisation, may begin outsourcing activities that are closely tied to core operations and the responsibilities of regulated entities.

Free flow of data across arms/blurred data boundaries

Conglomerates' ecosystems thrive on integrated data flows. However, when sensitive consumer information moves seamlessly across regulated and unregulated arms – through common access by designated personnel, absence of strict segregation, sharing between entities without customer consent or inadequate third-party sharing safeguards – risks proliferate. Thus, without clear purpose limitations, robust consent frameworks and segregated data storage, such flows create vulnerabilities around privacy, mis-selling and misuse. Reflecting this, regulators have signalled heightened scrutiny on data storage and flows through various regulatory mandates and inspection frameworks.

Tech platform concentration risks

Shared technology stacks can drive efficiency but introduce single points of failure. A cyber breach, system outage or vendor compromise may simultaneously disrupt multiple entities within a group. Thus, regulators emphasise resilience and avoiding redundancies, because centralised setups can often expose gaps when tested against stress scenarios at the entity level.

Co-mingling of funds

A recurring concern in multi-entity groups is the blurring of financial boundaries between regulated and unregulated arms. Lack of segregation of settlement accounts, float balances or customer funds can lead to the misuse of funds, liquidity shortfalls or the misrepresentation of solvency. Even indirect practices, such as pooling operational expenses or using a common treasury without robust reconciliation, can expose regulated entities to the risks arising from unregulated ones.

Customer protection and clarity of responsibility

From the customer's perspective, the rise of multiple entities and group structures, coupled with centralisation, has created confusion regarding 'who is actually responsible' for service delivery, dispute redressal and safeguarding of their interests.

A customer may sign up on a single interface for payments, insurance, investments and lending, but due to centralisation, servicing of such underlying products is often managed by an entity distinct from the one the customer originally engaged with. This creates confusion because, without adequate disclosure, customers may be unclear about aspects such as the following:

- which entity is the licensed service provider
- which entity owns their data
- who holds responsibility for grievance redressal
- where liability rests if there is a failure in service delivery

Regulators have emphasised the principle of 'clear attribution of responsibility' to protect customers from mis-selling, misinformation or denial of accountability. However, with the implementation of centralisation at the FSP and the resulting fragmentation of responsibilities, a lack of clarity in disclosures and uncertainty in grievance resolution.

In toto, while centralisation can improve efficiency, it may also encroach into areas that regulators have explicitly sought to restrict, raising concerns about whether accountability truly rests with the regulated entity.

5 Aligning business and regulatory expectations through the right roadmap

As India's financial ecosystem matures into multi-licensed conglomerates, the real question is no longer the speed of business growth but whether governance structures and regulatory guardrails will evolve in tandem. Aligning business ambition with regulatory expectations must be deliberate, ensuring that operational agility does not compromise fiduciary duties, customer protection and data security. In practice, when pursuing centralisation, this alignment can be achieved by adhering to the following key principles:

Core functions cannot be outsourced

For every regulated business, it is essential to clearly define core functions – activities that directly relate to the entity's purpose, fiduciary responsibilities, compliance obligations and, most importantly, decision-making authority. Regulators emphasise that core functions should remain in the licensed entity; however, there is no exhaustive or uniform definition of what constitutes a 'core function'. These activities vary across business models, product lines and operational setups, making it necessary for each entity to assess and define its own core functions. For instance, a FinTech regulated in the payments space would consider fiduciary activities such as funds handling, managing settlements and payment system operations (e.g. netting and settlement) and monitoring transactions management (e.g. reconciliation, reporting and item processing) as core functions. The overarching objective is that these functions should never be outsourced to ensure that accountability, governance and regulatory responsibility remain firmly within the regulated entity.

Let us consider the example of a question put forth for deliberation: Can the marketing function be centralised? The immediate reaction may be that it is non-core and hence can be entirely centralised. This conclusion is not entirely incorrect. However, the marketing function may entail some actions that arise from the regulatory requirements, such as disclosure for mutual fund distribution prescribed by the capital market regulator. While disclosures may very well be part of the centralised marketing or legal function and hence curated by them, the content of such disclosure requires review and approval from the relevant decision makers at a regulated entity. Moreover, such disclosures should also be seen to be from the regulated entity even if powered by the centralised marketing team at the back end.

Segregated governance, common oversight

To maintain integrity in governance while benefitting from centralised operations, certain governance-related guardrails must be implemented at the level of the regulated entity:

- Key regulatory roles for a particular entity or business model in the FSP should be designated within the regulated entity itself, not at a group level.
- Decisions relating to core functions must be retained within the regulated entity. While regulatory accountability lies within each regulated entity, some oversight and guidance may come from centralised teams
- Policies and structures should prevent conflicts of interest, ensuring that pursuing operational efficiency does not compromise the entity's integrity or core operations. Regular audits should be conducted to ensure that shared services, centralised functions or group-level support do not blur the accountability of regulated entities.

Governance should be treated as a strategic imperative, not just a compliance afterthought. Boards and senior management must actively ensure that the segregation between regulated and unregulated activities is maintained and operationalised in everyday decision making.

Data governance and technology controls

Shared data and technology stacks form the backbone of centralisation; however, they also constitute the largest potential risk. Therefore, effective data and technology governance requires the following:

- Segregated, purpose-driven data handling and access: Any data collected, stored, shared and accessed should serve clearly defined business purposes, with strong separation to ensure secure and controlled access.
- Explicit customer consent: Data collection, sharing and storage must be governed by transparency – that is, by obtaining explicit consent.
- Entity-level resilience protocols: Redundancy, disaster recovery and security testing should be scoped at the level of each licensed entity, not just at the group level, to mitigate concentration of risk.
- Prompt data access: Each data structure, process and flow should reinforce external stakeholders' trust in the entity. For stakeholders such as regulators and customers, robust data protection and access are non-negotiable pillars of data-related centralisation.

Customer interface

In the present day scenario, typically, if a customer is a customer of an FSP, it is likely that they would have availed multiple financial products through the relevant FSP. As a result, an FSP would naturally prefer to cater to these customers through a centralised customer service desk for a more seamless experience. However, at times, this aspiration could have mixed results for the FSP. While some customers may be delighted to have a single interface for all their queries and grievances, others may be perplexed if they keep landing on a single common interface when they want to reach out to the financial product issuing entity. The latter issue is grave and has been a consistent sore point for regulators over the years. Due to this, FSPs may find it challenging to balance their own aspirations to centralise customer service (a resource-intense function) with the requirements of regulators.

These considerations make decisioning around centralisation of a particular function extremely contentious. A potential solution is to centralise initial query-based support (which is standard in nature) or recording of grievances. Subsequent customer escalations or support should be housed in the relevant financial product issuing entity.

Collaborative approach among responsible owners

Centralisation of activities should not be seen as shifting responsibilities to a few departments or individuals but as collaboration among them. Within the multiple activities that an entity may want to centralise, quite a few may require the coordination of people across functions and entities to ensure they holistically meet the accountability principles.

To elaborate on this point, using the previously mentioned marketing example, compliance with a single mandated disclosure involves drafting by the in-house lawyers from a legal perspective, review and approval by the compliance team and market outreach by the marketing team. These functions, whether centralised, decentralised or located in different entities (centralised, regulated, etc.), must operate together to ensure that there are no misses due to oversight that could lead to regrettable, irreversible outcomes. Therefore, while determining the functions and activities to be centralised and chalking out the implementation plan, identifying the responsible owners for each function and activity needs meticulous thinking.

Continuous monitoring and adaptive governance

Alignment is not a one-time exercise. As business models evolve, FSPs must continuously monitor the effectiveness of their centralised plans while keeping pace with the following:

- product offerings and the entity and its governance structure
- regulatory updates and regulator's expectations
- industry practices
- data and technology risks, etc.

6 Towards building resilient and compliant business models

As India's financial ecosystem continues to evolve, the path ahead requires a nuanced understanding of the multiple factors that influence decisions around centralisation and operational design. While centralisation can be an attractive lever for efficiency, it is not without its complexities, as highlighted above. Stakeholders, business models and the nature of activities vary significantly across entities, and these parameters must be carefully considered while engaging in strategic decision making. A one-size-fits-all approach across FSPs is not feasible.

Additionally, for non-regulated functions, pooling resources or streamlining operations is relatively straightforward. However, when regulated entities are involved, the stakes are far higher. Poorly designed centralisation can compromise compliance, erode entity-level independence and create unintended contagion risks. Thus, each decision to centralise core or sensitive functions must be deliberate, guided by clear principles and aligned with regulatory requirements and internal governance expectations.

The customer is at the core of this entire framework. Financial users in India, many of whom are unfamiliar with sophisticated technology or new to using digital means to avail financial services, place their trust in these systems. Even minor lapses in governance, clarity or accountability can undermine this confidence, pushing customers towards legacy in-person experiences. Therefore, ring-fencing is not just a regulatory requirement but also a guarantee of rendering a consistently delightful customer experience.

In summary, the way forward demands a careful balancing act: leveraging centralisation to increase operational efficiency while embedding governance and risk management at all levels, with customer experience as the ultimate guiding principle. When carefully executed, this approach is expected to enable FSPs to scale, innovate and remain agile without compromising on compliance, accountability and customer trust.

About PwC

We help you build trust so you can boldly reinvent

At PwC, we help clients build trust and reinvent so they can turn complexity into competitive advantage. We're a tech-forward, people-empowered network with more than 370,000 people in 149 countries. Across assurance, tax and legal, deals and consulting we help build, accelerate and sustain momentum. Find out more at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

Contact us

Anshul Jain
Partner, Deals
PwC India
jain.anshul@pwc.com

Vivek Belgavi
Partner, Financial Services
PwC India
vivek.belgavi@pwc.com

pwc.in

PS/October 2025 - M&C 48878