Risk-Based Supervision for Inclusive Digital Financial Services

TRANSCRIPT: Introduction to Prudential Supervision

Digital Financial Services providers offer diverse services through a variety of delivery channels, such as online branches, mobile offices, and agents. These diverse offerings require the use of IT systems and telecommunications to connect payment infrastructures, such as switches and other payment systems. DFS providers also engage in business partnerships, outsourcing arrangements, and often participate in data sharing schemes, such as open banking and open finance. Some DFS providers are adopting novel business models, such as banking-as-a-service or specialising in niche pieces of the financial value chain in module business models.

All these innovations pose prudential risks. These are risks that jeopardise the soundness and safety of the DFS provider. Such risks include operational risk, liquidity risk, and loss of customer funds. These also pose prudential risks to the financial institutions that partner with the DFS provider, such as third-party risks and business continuity risk.

Prudential risk could also increase other risks for DFS providers, such as money laundering and terrorism financing, and consumer risks.

When assessing risks, supervisors need to consider the DFS providers' activities, as these will define the inherent risk for the DFS provider, which, in turn, will determine the supervisory model that the supervisor will need to develop to appropriately supervise the specific provider.

Nowadays, DFS providers span many types of regulated activities, including:

- deposits and payments,
- credit,
- insurance, and
- virtual assets, which are becoming more and more common in emerging economies.

Most of these activities, when offered by traditional financial institutions, such as banks, are already subject to prudential regulations.

For DFS providers, similar provisions apply, including:

- minimum entry capital,
- fit and proper requirements,
- governance requirements,
- requirements for internal controls, and
- risk management.

These requirements differ across regions. Initial capital requirements, for example, vary widely from one country to another. In addition to these provisions, there are requirements that are specific to some financial risks depending on the type of activities the provider offers.

For a **digital lender**, the main financial risk will be credit risk. Depending on the mix of activities this provider engages in, its credit risk will be regulated via provisions such as:

- concentration limits (when a single borrower cannot borrow more than a certain amount),
- risk classification rules,
- loss provisioning rules, and
- limits to related party lending, among others.

For a **digital insurance provider**, the main risk will be insurance risk. This is the risk of a covered event actually happening, such as the death of a life insurance policy holder. An insurance company is heavily regulated on how they manage their financial resources and are required to keep technical reserves to cover their risk.

For a **payment service provider**, including e-money or mobile money provider, the main risk will be operational risks and the specific risks of payment activities, including settlement risk. The providers will be subject to various technical safeguards in payments regulations, to help mitigate these risks. When DFS providers are allowed to combine different activities, such as deposit taking and lending, their inherent risk increases considerably. This requires regulation and supervision to be stricter to mitigate the associated risks.

This is why some types of entities that collect deposits from the public are subject to capital adequacy requirements. This is when regulation requires DFS providers to leave a cushion to absorb potential losses.

Regulation and supervision must be proportional to the risks and opportunities posed by different types of DFS providers from a prudential perspective.

Two of the most significant risks for DFS providers, that require focus for prudential supervision, are operational risk and the risk of money laundering and financing of terrorism.

Operational risk is a significant prudential risk that most DFS providers face. The Basel Committee on Banking Supervision defines it as 'the risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events'.

Regulations often include general requirements for DFS providers to manage their operational risk. Such regulations cover requirements for risks related to fraud, agents and other third parties, cyber threats, IT systems, and business continuity.

Agent-related risks may be one of the main components of the operational risk for certain types of DFS providers, namely non-bank e-money issuers and money transfer operators that specialise in remittances.

The agility of Digital Financial Services can help fight against the risks associated with **money laundering and financing of terrorism**, while, at the same time, increasing these risks. Increasing digitalisation of transactions in the financial sector makes ML/FT transactions more traceable, when compared to cash. This is one of the most important areas for supervisors who are concerned about balancing risk mitigation with financial inclusion. When disproportionality is applied, controls and rules related to anti-money laundering and countering the financing of terrorism can become a major obstacle for financial inclusion.