DIGITAL FINANCIAL TRANSFORMATION

Diagnostic Assessment and Action Plan for Inclusive Digital Infrastructure for the Next Level of Sustainable Development in South Asia

SPECIAL REPORT

CONTENTS

EXECUTIVE SUMMARY	3
1. INTRODUCTION	4
2. DIAGNOSTIC REVIEW OF REGIONAL STATUS: INCLUSIVE DIGITAL INFRASTRUCTURE, FINANCIAL INCLUSION, AND DIGITAL FINANCE	8
3. INCLUSIVE DIGITAL INFRASTRUCTURE: BENCHMARKS FOR THE NEXT LEVEL OF INCLUSIVE GROWTH AND DEVELOPMENT	20
4. MAJOR ACTION RECOMMENDATIONS: MEDIUM-TERM (THREE TO FIVE YEARS) - BUILDING CAPACITY OF REGULATORS, INDUSTRY AND CONSUMERS	25
5. MAJOR ACTION RECOMMENDATIONS: MEDIUM-TERM (THREE TO FIVE YEARS) - TOOLS FOR REGULATORS	31
6. MAJOR ACTION RECOMMENDATIONS: MEDIUM-TERM (THREE TO FIVE YEARS) - THE NEXT LEVEL OF IDI	33
7. BUILDING A REGIONAL CROSS-BORDER STRATEGY	39
8. CONCLUSION	40
BIBLIOGRAPHY	42
ACRONYMS	45
ANNEX A: SURVEY QUESTIONS FOR A COMPREHENSIVE DIAGNOSTIC ASSESSMENT OF SARFII MEMBERS' DIGITAL ECOSYSTEMS	47
ANNEX B: LIST OF NON-SARFI MEMBER ORGANIZATIONS WHOSE INPUT WAS TAKEN DURING IN-COUNTRY VISITS (EXCLUDING SURVEY PARTICIPANTS)	49

ACKNOWLEDGMENTS

This special report is a product of the South Asian Region Financial Inclusion Initiative (SARFII) and members of its Task Force.

Contributors:

From the SARFII Task Force: Shubhash Chandra Ghimire (Director, Payment Systems Department, Nepal Rastra Bank), Masuma Sultana (Director, Payment Systems Department, Bangladesh Bank), Kesang Jigme (Director, Department of Payment & Settlement Systems, Royal Monetary Authority of Bhutan), Ahmad Nazeeh Mohamed (Manager, Payment Systems and Oversight Division, Maldives Monetary Authority), Ahmed Sumair (Joint Director, PSP & OD, State Bank of Pakistan), and Kanchana Ambagahawita (Deputy Director, Payments and Settlements Department, Central Bank of Sri Lanka).

From the AFI Management Unit: Ali Ghiyazuddin Mohammad (Head of Policy Management, Policy Programs & Implementation).

Our special thanks to Syed Musheer Ahmed (Founder and MD, FinStep Asia), Douglas Arner (Kerry Holdings Professor in Law and RGC Senior Research Fellow in Digital Finance and Sustainable Development, University of Hong Kong; Sir Roy Goode Chair, Queen Mary University of London; Associate Director – Research, Cambridge Centre for Alternative Finance), Kuzi Charamba (Founder and Chief Executive Officer, Tese); Sangita Gazi (Post-Doctoral Research Fellow, the Wharton School, University of Pennsylvania), and Monica Jasuja (Payments and Product Strategy Advisor) for their support in researching and drafting the report.

We would also like to thank AFI member institutions, partners, and donors for generously contributing to the development of this publication.

This report is funded with UK aid from the UK government.

Cover photo: Woman selling vegetables on the street market in Leh Ladakh / Shutterstock

EXECUTIVE SUMMARY

This report presents the findings of an Alliance for Financial Inclusion (AFI) research project reviewing the status of financial inclusion and inclusive digital infrastructure (IDI) among AFI's South Asia members, as part of the South Asian Regional Financial Inclusion Initiative (SARFII). The project aimed to assess both opportunities and needs to advance the next level of inclusive sustainable development in the region and to develop strategic recommendations focused on IDI to support the objectives of members to improve financial inclusion, inclusive growth, and sustainability.

From November 2024 to May 2025, the project conducted a comprehensive diagnostic review of the evolution of financial inclusion and the role of technology, particularly digital and financial infrastructure, across the region and internationally. The team then engaged with members of AFI's SARFII Payments Expert Group (PEG), who led and supervised the project, in a series of online and in-person meetings with stakeholders in Nepal, Sri Lanka, and India. A survey was also developed and circulated with PEG members to gather input from digital finance ecosystem stakeholders in each country.

Drawing on desk research, meetings, and survey responses, the report first summarizes the evolution and current state of financial inclusion and IDI across the region (Section II). Section III synthesizes key benchmarks for IDI and digital financial transformation, based on AFI's FinTech for Financial Inclusion Strategy (FT4FI)[1] and related IDI experiences globally. Sections IV, V, and VI present the main recommendations for SARFII members to guide future interventions over the next three to five years. Section VII offers suggestions for regional-level activities under SARFII, while Section VIII summarizes strategic recommendations for each individual member.

1 Alliance for Financial Inclusion. 2018. FinTech for Financial Inclusion: A Framework for Digital Financial Transformation. Available at: https://www.afi-global.org/publication/fintech-for-financial-inclusion-a-framework-for-digital-financial-transformation/

Michele Burgess / Alamy Stock Photo

1 INTRODUCTION

Financial inclusion has rapidly expanded over the past decade in South Asia,[2] underpinned by significant advancements in digital payments and foundational inclusive digital infrastructure (IDI). This is reflected by the widespread adoption of diverse digital payment platforms and a doubling in transaction volumes over the past five years. Authorities across the region have also progressed in advancing digital identification systems, supported by increasingly supportive regulatory and policy frameworks across a broad spectrum of digital financial services (DFS).

Against this backdrop, the Alliance for Financial Inclusion (AFI) launched this project under the South Asian Regional Financial Inclusion Initiative (SARFII), which brings together central banks and regulators from Bangladesh, Bhutan, the Maldives, Nepal, Pakistan, and Sri Lanka. This project reviews the progress in financial inclusion across SARFII members and identifies opportunities to support the next stage of inclusion and sustainable development through IDI over the coming three to five years. Building on its previous work,[3] the research team, comprising AFI management team members and a team of experts, worked closely with the SARFII Payments Expert Group (PEG) and engaged stakeholders from each country's digital financial ecosystem, as well as India, over a six-month period (November 2024 to May 2025).

The first phase involved a comprehensive review of existing research, data, and regional and global experiences on financial inclusion, sustainable development, and IDI, providing a baseline for in-depth country analysis. Following this, the team worked closely with PEG members (see Annex A) to conduct consultations with institutional teams working on financial inclusion, payments, digital finance, consumer protection, cybersecurity, legal and regulatory affairs, and policy strategy. Insights from these discussions were then synthesized to create a diagnostic assessment of the current landscape across SARFII members.

A regional survey was also developed with PEG members and distributed to ecosystem stakeholders in all SARFII countries, receiving over 40 responses (Annex A), complemented by in-person consultations with stakeholders in Sri Lanka, Nepal, and India (Annex B). The cumulative findings were presented at the February 2025 SARFII regional meetings in Kathmandu. This report presents the overall findings and recommendations, while country-specific recommendations developed separately with each member are not included.

The study finds that digital payments and IDI were central to expanding financial inclusion across the region, and highlights a significant opportunity to build on these first-generation gains through second-generation strategies in digital finance, FinTech, and IDI. While new risks have emerged, particularly in cybersecurity and consumer protection (described here as the "democratization of digital financial crime"), regional and global experiences point to a path forward for SARFII members to deepen inclusion and sustainability over the next three to five years through more advanced and targeted strategies.

This report highlights the current regional context for financial inclusion, digital finance, and IDI in Section II. Section III sets benchmarks for advancing to the next level, identifying key elements of first and second-generation strategies. Sections IV and V outline strategic priorities for individual SARFII members, while Section VI identifies opportunities for regional cooperation at the regional level to support inclusive, sustainable development, and IDI advancement both within SARFII and across AFI more broadly.

Andrii Shevchuk / Alamy Stock Photo

2 Comprising of Bangladesh, Bhutan, India, the Maldives, Nepal, Pakistan, and Sri Lanka.

3 Note: the previous work mentioned consisted of a Payment Study.

SUMMARY OF CURRENT STATUS

SARFII members have made key strides in advancing financial inclusion and sustainable development through DFS, FinTech, and IDI strategies, though challenges remain in fully leveraging DFS to build inclusive financial systems.

First, digital ID systems are not consistently integrated with banking and FinTech services. Fragmented e-KYC processes and delays in issuing comprehensive digital ID regulations impede swift, paperless onboarding. While digital finance usage has grown in volume and value, DFS still often operates in silos, limiting seamless user experiences across systems.

Second, cash remains dominant in several member countries, with cash-to-GDP ratios nearing or exceeding 10 percent.[4] Structurally, urban-rural divide persists in cash use, internet access, and mobile connectivity. Despite high mobile penetration, uneven internet availability and infrastructure, along with rural reliance on cash, continue to slow digital adoption even as urban areas rapidly embrace digital technologies.

Third, limited digital literacy, smartphone penetration, and infrastructure in remote areas continue to restrict access to digital ID and DFS, disproportionately affecting women and traditionally excluded groups.

Finally, high transaction costs and fee structures discourage low-income users and small merchants from full digital uptake. Though SARFII member countries have developed digital payment regulations over the past decade, the digital financial landscape continues to evolve. Emerging issues include data laws and regulations (e.g. open banking/finance and AI), digital lending laws, regulatory technology (RegTech), supervisory technology (SupTech), and growing risks in cybersecurity and consumer protection.

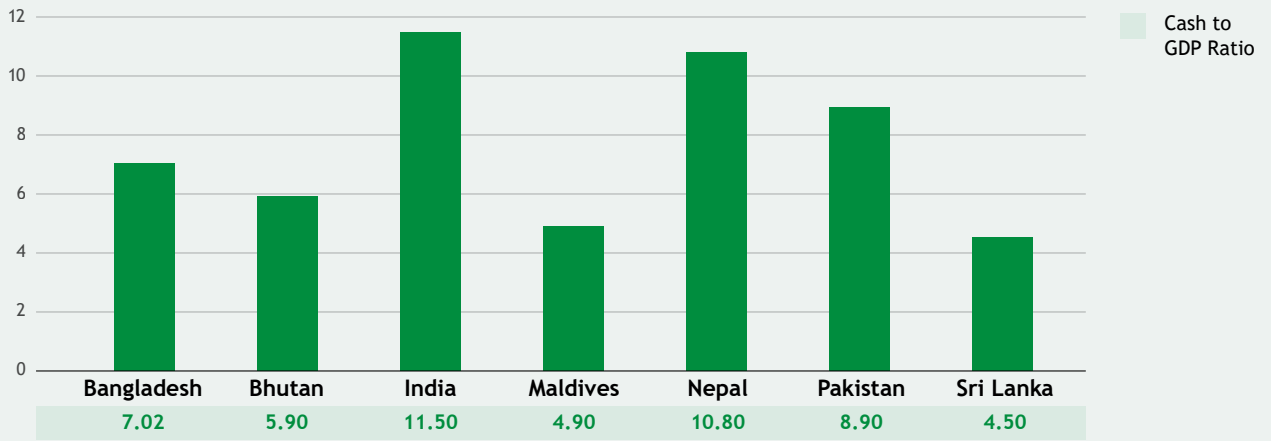
Regulators in member countries have strengthened consumer protection and cybersecurity through measures which include digital literacy programs, IT governance frameworks, regular audits, and cyber incident response protocols. The region reports relatively low rates of technical cyber breaches, reflecting strong collective efforts. Countries, including Bangladesh, India, and Pakistan score well in cybersecurity readiness.[5] Member states are also expanding programs to further increase digital finance access for women and vulnerable groups, underlining their commitment to inclusive growth.

Further improvements are needed despite these advancements. Consumer confidence can be strengthened through more integrated dispute resolution mechanisms and broader financial literacy outreach. The regulatory environment remains fragmented, with a need for unified data protection laws, and better alignment across multiple regulations to support innovation. Scams and fraud, particularly affecting women, older populations, and rural communities, continues to erode trust, which requires expanding targeted educational programs to reshape consumer behavior and increase adoption. Ongoing reforms, such as the introduction digital-only bank licenses, FinTech licenses, and comprehensive cybersecurity guidelines, are key to ensuring a cohesive, inclusive, and secure digital finance ecosystem across the region.

4 Based on cash in circulation to nominal GDP for each country for 2023/24 – Central Bank statistics and authors' calculations (Currency in circulation/GDP).

5 Global Cybersecurity Index. 2024. Available at: https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

FIGURE 1: CASH TO GDP RATIO



SUMMARY OF KEY ACTION PLAN RECOMMENDATIONS

Drawing on the baseline review of experiences from other regions, notably the implementation of AFI's 2018 Sochi Declaration and FinTech for Financial Inclusion Strategy (FT4FI), as well as country-level strategies aligned with FT4FI and a review of SARFII's current digital finance and IDI landscape, the following priorities were identified to advance financial inclusion and digital infrastructure in the region over the next three to five years:

IMPLEMENTING DIGITAL FINANCIAL INCLUSION AND FIRST-GENERATION IDI STRATEGIES

- Develop second-generation national roadmaps for financial inclusion, digital finance, or payments with clear, time-bound KPIs for central IDI components.
- Advance the digitalization of government payments and receipts across sectors.
- Where not yet in place, support the development of a fully interoperable electronic payments system with Open APIs, around the clock availability, and participation by all licensed FSPs, alongside a national real-time gross settlement (RTGS) system.
- Reinforce principle-based policies and risk-based licensing for all digital financial services, including dedicated frameworks for standalone FinTech operators that promote innovation while safeguarding consumers and financial stability.
- Launch targeted financial literacy and capacity-building programs to empower women and rural entrepreneurs.
- Promote partnerships among financial institutions, telecoms, and FinTechs on joint digital literacy and consumer protection campaigns.
- Consider creating a public-private fund focused on consumer protection and financial literacy, with contributions from regulators and industry stakeholders.

ENHANCING DIGITAL IDENTITY AND KYC

- Expand adoption of secure, inclusive digital ID solutions and integrate them into centralized e-KYC repositories, paced to the maturity of the digital ecosystem.
- Strengthen shared KYC frameworks to streamline customer onboarding and improve the efficiency of FSPs.
- Consider tiered, risk-based KYC and account types, such as basic digital wallets and full-service bank accounts, reflecting different levels of functionality.
- Deploy mobile and offline verification tools to bridge rural connectivity and digital literacy gaps.
- Work with government agencies to establish a digital MSME ID for use in banking, payments, and credit services.

DEVELOPING SECOND-GENERATION IDI

- Develop Open Banking and Open Finance frameworks to integrate financial services with sectors such as e-commerce, asset purchasing, and utilities, initially for domestic use, with the potential for regional integration.
- Enable data-driven digital lending and support digital credit platforms that ensure responsible lending and use alternative data for credit risk assessment.

REGULATORY AND GOVERNMENT INITIATIVES

- Adopt innovative and flexible regulatory models, including test-and-learn approaches and regulatory sandboxes to run Proof of Concepts (PoCs), supported by dedicated FinTech engagement teams.
- Leverage government programs to increase account onboarding and financial literacy, including public education on budgeting, saving, and investing.
- Consider establishing Self-Regulatory Organizations (SROs) for under-regulated sectors such as digital lending and virtual assets, while facilitating FinTech industry associations. Ensure that frameworks allow for meaningful enforcement.
- E stablish inter-agency councils to improve dialogue and coordination and implement continuous review mechanisms to adapt to emerging technologies.
- Invest in advanced RegTech and SupTech solutions for real-time compliance monitoring and risk management.
- Build public–private partnerships to subsidize last-mile connectivity and upgrade legacy IT systems of banks and enterprises.

CYBERSECURITY AND CONSUMER PROTECTION

- Mandate AI-driven fraud detection, multi-factor authentication, and regular cybersecurity audits across all financial institutions, covering both mobile payments and digital banking services.
- Improve inter-agency threat coordination through joint operations centers for real-time intelligence sharing and rapid incident response.
- Implement comprehensive consumer protection frameworks tailored to the evolving risks in each country.
- Launch consumer fraud reporting portals to streamline fraud case reporting, facilitate dispute resolution, and enable aggregated data collection for stakeholders.
- Track and report metrics on impacts from fraud, including transaction volumes and value.

Pierre Rochon / Alamy Stock Photo

2. DIAGNOSTIC REVIEW OF REGIONAL STATUS: INCLUSIVE DIGITAL INFRASTRUCTURE, FINANCIAL INCLUSION, AND DIGITAL FINANCE

To understand the current state of financial inclusion and inclusive digital infrastructure across SAFRII member countries, the study began with a process of external and internal baselining. As outlined earlier, this process aimed to clarify the status of digital finance, FinTech, and IDI across the region and focused on six major areas covered in this section: digital payments and financial services (section A), digital identification and account access (section B), mobile access and data infrastructure (section C), consumer protection and cybersecurity (section D), SME finance and financial inclusion (section E), and legal and regulatory frameworks (section F).

A. DIGITAL FINANCIAL INCLUSION: DIGITAL PAYMENTS AND FINANCIAL SERVICES

South Asia's digital financial transformation is reflected in the rapid expansion of digital payments and increased adoption of mobile-based transactions. For example, Bangladesh has developed extensive mobile financial services (MFS), while Pakistan has achieved record transaction volumes through its branchless banking regime, established in 2008, and Raast Instant Payment System, which launched in 2021. Raast has over 43 million registered users and has processed more than 1.5 billion transactions worth PKR34.5 trillion to date, now averaging five million transactions daily (60 percent of retail fund transfers). The system currently processes transactions exceeding PKR1 trillion in value every 10 days.[6]

India's Unified Payments Interface (UPI), launched in 2016 alongside Digital India and India Stack initiatives, has brought hundreds of millions of previously unbanked citizens into the financial system. Regional efforts, such as the UPI-Nepal Payment Interface (NPI) integration, reflect growing cross-border interoperability in creating instant, secure digital payment systems.[7]

The region is experiencing both growth in transaction volume and diversification in payment innovations. Sri Lanka has introduced payment platforms based on CEFTS, its Instant Payment System, enhancing user convenience and security, while Bhutan uses a regulatory sandbox to support FinTech innovation. In Nepal and Pakistan, QR-based payment systems are replacing cash transactions and extending financial services to underserved populations.

The Maldives, with its Favara instant payment system and as the first South Asian country to launch 5G connectivity, continues to improve mobile penetration and connectivity.[8]

Despite progress, four major challenges persists:

I. TACKLING THE DIGITAL DIVIDE

Fragmented systems hamper interoperability and the user experience, limiting the central advantage of network effects and slowing adoption. Outreach and education efforts remain restricted, and uptake of digital finance tools is hindered by low financial and digital literacy, poor risk awareness, and limited connectivity in remote areas. Urban-rural disparities remain particularly stark, as urban centers rapidly adopt digital tools while many rural areas continue to depend on cash transactions. This divide also extends to mobile phone and internet access, despite overall high penetration rates.

For example, while Bangladesh has an over 100 percent mobile phone penetration,[9] only 61 percent of people own smartphones according to the BRAC Institute of Governance and Development, and just 2.4 percent of rural households have computers.[10] Internet use is

6 As noted by the State Bank of Pakistan.

7 The Kathmandu Post. Digital penetration in Nepal's geopolitics. 2023. Available at: https://kathmandupost.com/columns/2023/06/17/digital-penetration-in-nepal-s-geopolitics

8 International Finance Corporation. 2023. Connecting the Unconnected - Transforming Digital Infrastructure in the Maldives. Available at: https://www.ifc.org/en/stories/2023/connecting-the-unconnected-in-maldives#:~:text=While%20Maldives%20has%20made%20substantial,quality%2C%20reliability%2C%20and%20affordability

9 GSMA. GSMA Mobile Connectivity Index 2024. Available at: https://www.gsma.com/r/wp-content/uploads/2024/10/The-State-of-Mobile-Internet-Connectivity-Report-2024.pdf?utm_source=website&utm_medium=button&utm_campaign=somic25

10 BIGD. 2019. Digital Literacy and Access to Public Services in Bangladesh. Available at: https://bigd.bracu.ac.bd/study/digital-literacy-and-access-to-public-services-in-bangladesh/

similarly split, with 36.5 percent in rural areas versus 71.4 percent in urban areas based on a Bangladesh Bureau of Statistics survey.[11]

The disparity in infrastructure and limited high-speed internet access continue to constrain digital payments in rural areas lacking traditional financial systems. In India, 40 percent of urban adults use digital payment accounts compared to 30 percent in rural households, while in Bhutan, two-thirds of the urban banked population use mobile banking versus just one-third of rural users.[12]

Gender disparities compound the digital divide. In the Maldives, adolescent girls lag boys in acquiring basic digital skills.[13] While internet awareness in Bangladesh is nearly equal between women (73 percent) and men (71 percent),[14] 37 percent of female mobile money users require assistance, as opposed to 25 percent of men. In India, the gap is 47 percent of women versus 17 percent of men, and in Pakistan, 44 percent versus 18 percent.[15] The 2025 Mobile Money Report attributes this lack of digital skills to the widening gender gap in MFS.[16]

The following graphs summarize the evolution of major international baseline indicators across the region on account access, gender gaps, and digital payment activity.[17] The major international data sources are included for context, though the most recent World Bank Global Findex only covers data up to 2021. The next update is expected in mid-2025, but significant developments, often driven by IDI strategies, have taken place across the region over the past three years, as discussed further in the following sections.

11 The Daily Star. 2025. Internet shows stark rural-urban divide. Available at: https://www.thedailystar.net/business/news/internet-shows-stark-rural-urban-divide-3789861

12 Royal Monetary Authority of Bhutan. Access to Finance – Demand Side Survey 2022. Available at: https://www.rma.org.bt/bank/RMA%20Publication/papers/2023/Access%20to%20FInance%20Demand%20Side%20Survey%20Report%202022.pdf?utm_source

13 Greater Internet Freedom. n.d. Mitigating Digital Divide Impact on Marginal Groups in the Maldives. Available at: https://greaterinternetfreedom.org/blog/mitigating-digital-divide-impact-on-marginalized-groups-in-the-maldives/#:~:text=SPD%20also%20organized%20awareness%2Draising,raising%20awareness%20about%20digital%20rights

14 World Wide Web Foundation. Women's Rights Online Report Card – Bangladesh. 2020. Available at: https://webfoundation.org/docs/2020/09/Digital-Gender-Audit-Scorecard-Bangladesh-Final-Sept-2020.pdf

15 GSMA. The State of the Industry Report on Mobile Money 2025. Available at: https://www.gsma.com/sotir/wp-content/uploads/2025/04/The-State-of-the-Industry-Report-2025_English.pdf#page=9.03

16 Ibid.

17 Global Findex 2021, IMF Data 2023, Central Banks' Data, GSMA Report, Data Portal Report, National Telecom Authorities. Note: The gender gap in accounts for India and Sri Lanka is 0%. Mobile Money Accounts, IMF data was unavailable for Bhutan and Sri Lanka for 2023.

FIGURE 2: KEY METRICS

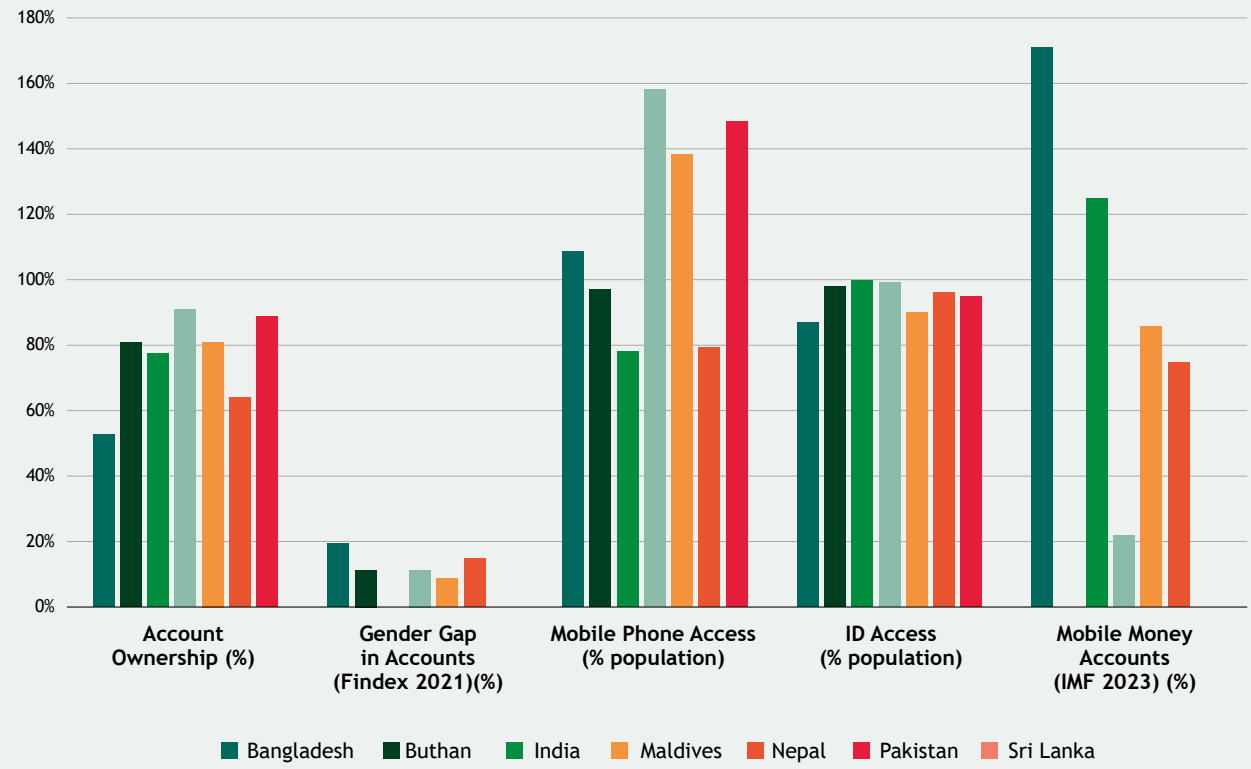


FIGURE 3: ACCOUNT OWNERSHIP[18]

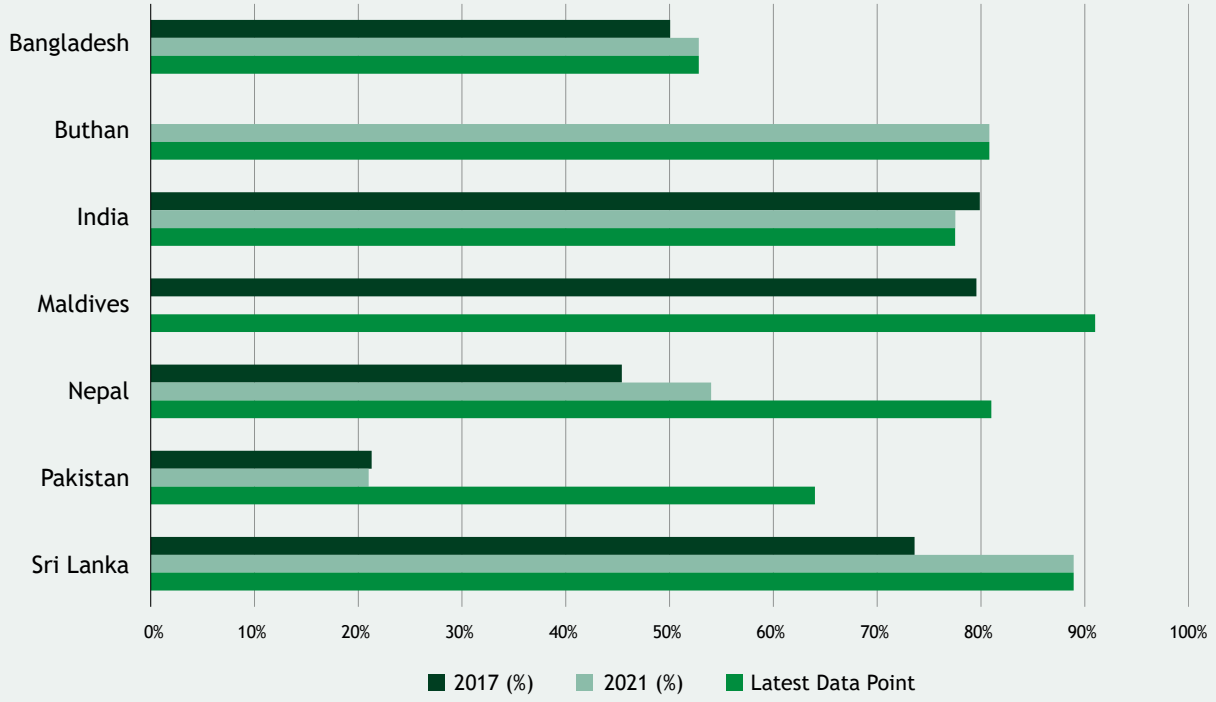
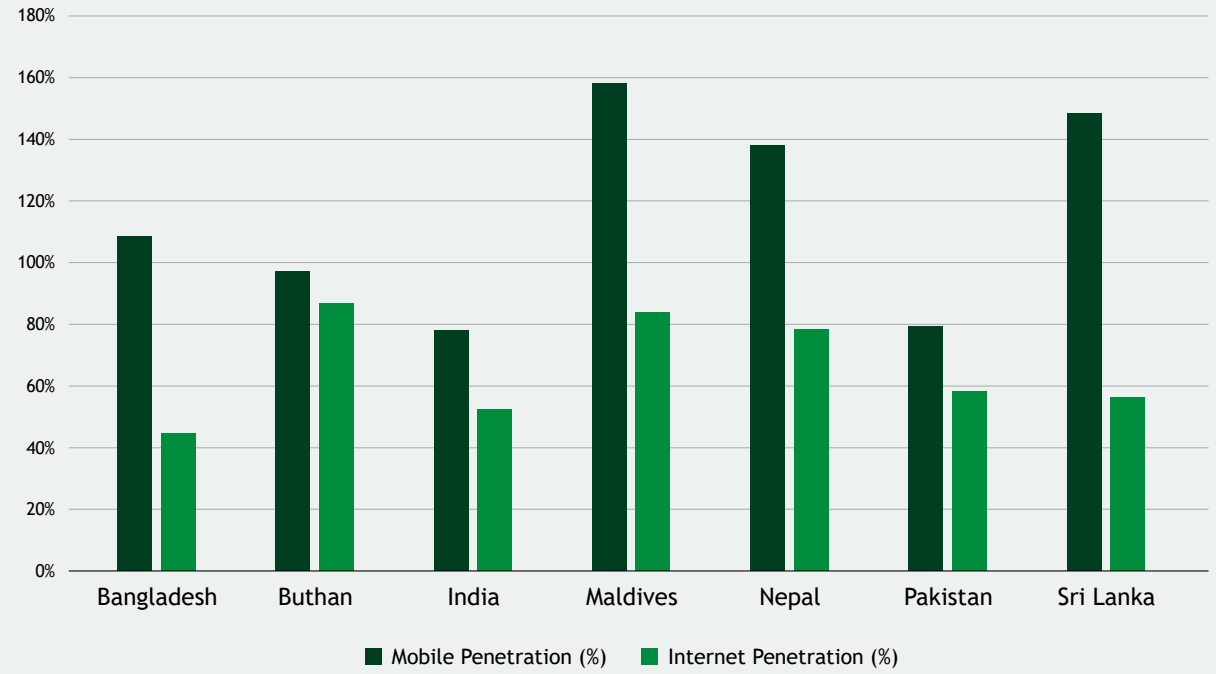


FIGURE 4: DIGITAL INFRASTRUCTURE[19]



18 Data for 2017 and 2021 are largely from the Global Findex, while the latest data points are either the last Findex data point or latest published data from the central bank or IFC from 2023-24.

19 GSMA Annual Report, DataPortal 2023, National Telecom Authorities. Note: Mobile penetration exceeds 100% because many individuals use multiple SIM cards or mobile connections.

Godong / Alamy Stock Photo

The digital divide is further exacerbated by affordability issues in some countries, where the high cost of broadband and advanced network services limits access for low-income users, restricting their ability to use internet-based financial services. Bhutan, for example, faces higher internet costs than others in the region and has recently pledged to reduce them.[20] Bangladesh imposes the highest consumer taxes as a share of the total cost of mobile ownership, with a 15 percent value-added tax, a 25 percent smartphone duty, and additional charges for SIM cards.[21] Relatively higher and complex transaction fees further deter low-income users and small merchants from fully shifting to digital systems.

II. ACCELERATING GENDER PARITY

While countries like Sri Lanka have achieved gender parity in account access and Bhutan has made significant progress, women across much of the region still face lower account ownership and usage of DFS than men. In Pakistan, for instance, 32 percent of men have mobile money accounts compared to just nine percent of women, making women roughly 70 percent less likely to own one. In India, only seven percent of women hold such accounts, compared to 16 percent of men, reflecting a 56 percent gap. In Bangladesh, the MFS gender gap widened from three percent to 16 percent in 2024, with just 23 percent of women owning accounts versus 52 percent of men.[22] Additionally, account ownership does not always translate to agency, especially in rural areas, where women's accounts are often operated by male relatives, undermining the intent of financial inclusion in DFS. Focused initiatives are needed to empower women through tailored financial products, training programs, user education, and supportive policies that address sociocultural barriers.

III. CONSUMER TRUST IN DIGITAL INFRASTRUCTURE

Cost and trust remain major barriers to full digital adoption across South Asia. A rise in scams, particularly phishing and social engineering targeting untrained consumers, has undermined consumer confidence in digital services. Member countries exhibit varying levels of cyber resilience in their consumer protection frameworks. According to the ITU's Global Cybersecurity Index 2024, Bangladesh, India, and Pakistan are rated Tier 1 (role-model status), Sri Lanka falls into Tier 2, and Bhutan and Nepal are placed in Tier 3.[23]

IV. INFRASTRUCTURE AND TECHNOLOGY CHALLENGES

Legacy IT systems present another layer of complexity. Several financial institutions, especially traditional banks and some credit service providers in both urban and rural areas, still rely on outdated systems not optimized for modern, high-volume digital operations. Upgrading these systems, including core banking, digital verification, and transaction monitoring, is vital to improve service delivery, transaction speeds, and the integration of new technologies. The adoption of unified data platforms and real-time analytics can also drive efficiency for FIs and service providers by enabling smarter use of data to meet both regulatory and consumer needs.

20 Business Bhutan. 2024. Government commits to Reduce Internet and Data Costs by 50%. Available at: https://businessbhutan.bt/government-commits-to-reduce-internet-and-data-costs-by-50/

21 GSMA. 2021. Achieving mobile-enabled digital inclusion in Bangladesh. Available at: https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2021/03/Achieving-mobile-enabled-digital-inclusion-in-Bangladesh.pdf#page=15.23

22 GSMA. The State of the Industry Report on Mobile Money 2025 page 71. Available at: https://www.gsma.com/sotir/wp-content/uploads/2025/04/The-State-of-the-Industry-Report-2025_English.pdf

23 International Telecommunication Union. 2024. Global Cybersecurity Index 2024. Available at: https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf

Although the region is making significant strides in DFS and payments, sustained success will require addressing interoperability, rural inclusion, cost efficiency, and consumer trust. By aligning innovative payment technologies with inclusive regulatory frameworks and digital literacy through second-generation IDI strategies, the region can fully leverage the benefits of a cashless economy while ensuring that no segment of the population is left behind.

There is also a pressing need to strengthen offline digital solutions, particularly USSD-based solutions for non-smartphone users. The region has seen mixed success, with examples including the implementation of bKash in Bangladesh, UPI Lite in India, NamastePay in Nepal, and Easypaisa and Jazzcash in Pakistan.[24] These services can help bridge the gap, offering a cost-effective solution while infrastructure is upgraded.

Persistent digital divides call for targeted policy interventions alongside infrastructure improvements to ensure equitable digital access. Bhutan's NgulDumb initiative exemplifies this approach, promoting financial literacy among young adults and women through education on savings, credit, and investment.[25] Similarly, Pakistan's National Financial Literacy Program, led by the State Bank of Pakistan and partners, runs thematic awareness campaigns and operates multilingual call centers focused on financial literacy.[26] While high mobile penetration offers a strong foundation, the region must address connectivity gaps and legacy technology systems to fully advance inclusive digital finance. Moving the ecosystem forward will require a coordinated strategy from regulators and government agencies, combining infrastructure investments, rural outreach, and IT modernization to ensure equitable access to digital services.

B. DIGITAL IDENTIFICATION AND ACCOUNT ACCESS

Digital identification and simplified account access systems are essential to building an efficient and inclusive digital finance ecosystem. Across the region, governments and financial institutions are shifting from paper-based processes to fully digital onboarding through e-KYC procedures and the use of digital IDs.

In Bangladesh and Sri Lanka, high National ID (NID) coverage has helped expand digital access to financial services by enabling large segments of the population to be identified without cumbersome procedures, while Pakistan's high-level Computerized National Identification system is used to open all bank accounts and e-wallets, supporting wide scale digital inclusion.

Progress, however, remains uneven. India is advancing biometric-based digitalization of its NID system, while Bhutan has introduced an integrated National Digital Identity (NDI) framework[27] that consolidates various identity records to streamline access to banking, government, and other services. Similarly, Pakistan's NADRA system offers real-time biometric verification through APIs, allowing FIs to authenticate customers using both contact and contactless methods. In parallel, Nepal and Sri Lanka are streamlining account access by launching centralized and shared KYC projects with biometric verification. These initiatives speed up the onboarding process and enhance the user experience, while reducing fraud risks by ensuring more accurate and secure identity verification.

I. FRAGMENTATION IN DIGITAL ID SYSTEMS

Despite strong national coverage, the integration of digital ID systems with banking and FinTech services remains inconsistent. Many systems still operate in silos, creating fragmentation that slows down the paperless onboarding of new customers. In some cases, delays in issuing comprehensive digital identity regulations and fragmented e-KYC processes further impede progress, underscoring the need for more harmonized and interoperable systems across the region supported by targeted policies.

II. RURAL AND DEMOGRAPHIC BARRIERS

Rural and demographic barriers add another layer of complexity. In remote areas, inadequate infrastructure, lower smartphone penetration, digital literacy, and language barriers continue to restrict access to digital ID systems, leaving many reliant on paper-based processes. While urban centers benefit from robust digital networks and literacy programs, rural regions lag behind. Addressing these challenges requires targeted outreach efforts that expand infrastructure and educate users with the skills and confidence to navigate digital identity tools safely and effectively.

24 Nepal Rastra Bank. 2024. A Study Report on the USSD-based Payment System and its Regulations: Suggestions for Nepal. Available at: https://www.nrb.org.np/contents/uploads/2024/10/A-Study-Report-on-the-USSD-based-Payment-System-and-its-Regulations-Suggestions-for-Nepal-1.pdf; also see: State Bank of Pakistan. n.d. Branchless Banking Statistics (Jul-Sep 2024). Available at: https://www.sbp.org.pk/acd/branchless/Stats/Branchless%20Banking%20Statistics%20for%20Jul%20-%20Sep%202024.pdf

25 World Economic Forum. n.d. NgulDumb. Available at: https://www.weforum.org/projects/nguldumb/

26 As noted by the State Bank of Pakistan.

27 Druk Holding and Investments Limited. n.d. National Digital Identity (Bhutan NDI). Available at: https://www.dhi.bt/strategy/InvestmentStrategy/technology/national-digital-identity-(bhutan-ndi)

CASE STUDY: Maldives' eFaas[28]

eFaas, developed by the National Centre for Information Technology (NCIT), is the National ID system for the Maldives enabling users to verify their identity using a single digital credential, eliminating the need for multiple logins and physical documents. The system uses a consent-based data-sharing approach to ensure transparency in managing and exchanging personal data across government agencies and organizations and incorporates multi-factor authentication, including password-less options like QR codes and one-tap mobile access to reduce the risk of phishing and cyber threats.

eFaas is also accessible to foreign residents, who can create a verified digital ID using their work permits. Since its launch, the system covers over 70 percent of the Maldivian population[29] and supports nearly 140 government and public sector services, helping streamline access and administration. The regulatory landscape and data protection remain key priorities.

The Maldives Monetary Authority (MMA) is shaping eFaaS regulation around three pillars: consumer protection, eKYC regulations that recognize digital identities, and technology risk management.

Joint efforts are underway to maximize the reach of eFaas by engaging a broad range of public and private sector stakeholders in the digital infrastructure ecosystem:

- The NCIT and MMA collaborate to provide regulatory backing of digital IDs, facilitating their integration into financial and government systems.
- eFaas is being integrated by one bank and one payment service provider for customer onboarding.
- Non-bank players and mobile payment service providers are encouraged to leverage eFaas to offer secure and inclusive financial services.

28 eFaas. n.d. Your key to a digital Maldives. Available at: https://efaas.egov.mv/

29 MMTV. 2025. Government modernizes eFaas to integrate all state services. Available at: https://en.mmtv.mv/2098

Tibor Bognar / Alamy Stock Photo

CASE STUDY: Pakistan's Aasaan Mobile Accounts

Launched on 13 December 2021, ASAAN Mobile Account (AMA) is a joint initiative of the State Bank of Pakistan (SBP) and the Pakistan Telecommunication Authority (PTA) under the National Financial Inclusion Strategy (NFIS). It enables any Pakistani with a valid Computerized National Identity Card (CNIC) to open and operate a branchless banking account using any mobile phone — without internet access.[30] Accessible via *2262#, AMA eliminates the need for smartphones or physical bank visits, allowing users to choose from 13 participating banks and open an account digitally. Identity is verified through the CNIC, with secure PIN-based protection. By leveraging Pakistan's extensive mobile penetration, AMA overcomes geographical and infrastructural barriers to banking.

As of April 2025, the platform has facilitated over 12.5 million account openings and processed 29 million financial transactions worth PRK163 billion,[31] demonstrating the popularity of digital payments. It has also handled 58 million non-financial transactions, such as balance inquiries, mini-statements, and PIN management, highlighting its role as a comprehensive, accessible financial platform positively impacting underserved populations.

Asaan has significantly advanced financial inclusion by integrating unbanked rural residents, women, and daily wage earners into the financial ecosystem (over 32 percent of these accounts were opened by women[32]). Its design caters to underserved populations by supporting cost-effective and accessible digital payments, savings, and future access to micro-credit, all on basic mobile phones without internet. Despite its success, AMA faces some challenges. Many target users, especially women and those in rural areas, struggle to understand digital banking processes. Limited access to cash-out points, user dependence on agents, and concerns over fees or trust in digital systems hinder broader adoption while occasional service interruptions and USSD session failures discourage users. Furthermore, the platform currently lacks access to savings schemes, micro-credit, insurance, and investment options. Expanding AMA's impact will require continued regulatory oversight, greater user awareness, infrastructure upgrades, and integration with additional service providers.

30 Further information is available at: https://www.nadra.gov.pk/

31 Further information is available at: https://www.sbp.org.pk/Finc/AMAscheme.html

32 As noted by the State Bank of Pakistan.

C. CONSUMER PROTECTION AND CYBERSECURITY

Comprehensive consumer protection and robust cybersecurity are critical for building and retaining trust in digital financial systems. Regulators across the region are strengthening safeguards through initiatives such as Pakistan's Fair Treatment of Customers framework and similar tailored mechanisms in Sri Lanka and Bangladesh, aiming to ensure accessible complaint channels and effective dispute resolution. However, the fragmented nature of reporting systems presents a significant challenge, as consumer protection mechanisms are often spread across banking, insurance, FinTech, and securities sectors without a unified framework. This disjointed approach leads to inconsistent resolution processes and delays, ultimately eroding consumer confidence in digital financial services.

Nathan Dumlao / Unsplash

CASE STUDY: Building Trust in Pakistan's Digital Financial System

The SBP has developed a multi-pronged strategy to promote trust in digital financial services across several dimensions:

Strengthening the Regulatory Framework

The SBP has introduced robust regulations to ensure financial institutions implement effective controls against fraud. BPRD Circular No. 04 of 2023 outlines a clear liability framework assigning responsibility for fraud to issuers, acquirers, or customers, while also setting requirements for governance, management oversight, and operational safeguards.

Promoting Customer Awareness and Education

Recognizing that social engineering scams often target customers directly, the SBP prioritizes public education. Key initiatives include:

- Mandating banks to send free SMS and email alerts for all domestic and international digital transactions.
- Training POS retailers to prevent misuse of card data at unauthorized terminals.
- Informing customers that banks will never request sensitive information via phone or email.

Together with the Pakistan Banks' Association, the SPB also runs digital fraud awareness campaigns and requires banks to continuously educate their customers.

Enhancing Interagency Coordination

Given that digital fraud often exploits vulnerabilities in both banking and telecom systems, the SBP and the PTA have formed a joint committee to address cross-sector fraud. This group meets regularly to improve coordination and fraud prevention mechanism.

Consumer Protection Framework

The SBP's Consumer Protection Framework[33] ensures transparency, fairness, responsible conduct, and access to dispute resolution, and integrates the Sunwai Consumer Complaints Portal, which allows real-time, trackable complaint submissions and escalations; it also includes systemic monitoring and minimum rules for internal dispute resolution.

The goal is to reduce fraud and ensure consumers feel protected, which is essential to drive usage in DFS. This effort includes comprehensive guidelines to counter cyber threats and secure digital finance ecosystems from risks such as phishing, hacking, and data breaches, together with mandatory cyber security audits for banks and FinTechs and penalties for non-compliance with data protection requirements. Recently, the SBP established the Cyber Risk Management Department to supervise cyber risks among regulated entities and address digital financial fraud more cohesively. In collaboration with various partners, the SBP has also launched awareness campaigns through social media platforms such as Facebook, TikTok, and YouTube.

Recognizing that awareness is the first line of defense, the SBP has introduced multiple initiatives targeting different demographics to improve their understanding of DFS, user rights, and available protections. This includes educational programs and tools in both Urdu and English, covering topics such as the safe use of payment cards, avoiding identity theft, and fair debt collection guidelines. These efforts have been supplemented through books and videos campaigns on social media. Additionally, the SBP has issued guidelines to ensure accessible banking services for the visually impaired and senior citizens.

Conduct Assessment Framework for Banks

The SBP issued a conduct assessment framework (CAF) for banks to establish a periodic, reliable, and comparable diagnostic mechanism that supports their commitment to the fair treatment of customers and effective conduct of risk management. Banks and MFBs were advised to adopt the CAF from 1 January 2017 and to conduct assessments annually as of 31 December. [34]

33 Further information is available at: https://www.sbp.org.pk/cpd/cpd-intro.asp

34 Further information is available at: https://www.sbp.org.pk/cpd/2016/C3.htm

With increased digitalization and online activity, countries across the region are pursuing multiple strategies to counter increasingly sophisticated cyber threats and strengthen cybersecurity. Standard measures now include mandatory IT governance, cybersecurity frameworks, regular audits, and incident response protocols. Nepal has introduced enhanced Cyber Resilience Guidelines, while Bhutan and Pakistan have implemented advanced multi-factor authentication and real-time fraud detection mechanisms to protect institutions and consumers from threats like phishing, malware, and other complex attacks.

Tony Tallec / Alamy Stock Photo

CASE STUDY: Cyber Resilience Frameworks in Nepal

The rapid rise in digital finance adoption over the past decade has introduced new cybersecurity challenges in Nepal, including digital fraud, data breaches, and financial scams. In response, the Nepal Rashtra Bank (NRB) issued a set of Cyber Resilience guidelines in 2023,[35] along with oversight mechanisms to establish a robust framework for identifying, responding to, and recovering from cyber threats. These guidelines focus on risk identification and mitigation, incident response and recovery, and are built on the pillars of testing, situational awareness, and learning and evolving. They also outline best practices and set compliance and reporting standards for financial institutions.

Key regulatory guidelines include mandatory two-factor authentication to address limitations of SMS based-OTPs, increased minimum capital requirements for Payment Service Providers (PSPs) to ensure investment in advanced cybersecurity infrastructure, and requirements for regular cybersecurity audits and incident reporting through a newly developed centralized reporting system. These efforts are supported by the rollout of the National Payment Switch, which aims to standardize digital transactions, as well as policies promoting e-KYC, remote onboarding, and the inclusion of DFS-related safeguard measures in the Consumer Protection Act. Despite these advances, Nepal faces several challenges in fully implementing cyber resilience frameworks, which include the growing volume and sophistication of cyber threats across both traditional banking and emerging FinTech players, many of whom lack the governance capacity of licensed banks. In addition, limited digital literacy and poor internet access in rural areas make comprehensive consumer protection more difficult.

To address these challenges and evolving threats, the NRB needs to adopt a multipronged approach that expands public financial literacy programs on cyber threats and safe digital practices, strengthen staff training within the NRB and financial institutions, explore the use of a regulatory sandbox to enable controlled testing of innovations under its cybersecurity standards, and pursue collaboration with SARFII members to strengthen cross-border payment and remittance systems.

35 Further information available at: https://www.nrb.org.np/contents/uploads/2023/ 08/Cyber-Resilience-Guidelines-2023.pdf?fbclid=IwAR3TraGHdyQvoT1oaS3yZFEjc0ZjQZvpfOS8nIaf3CwTJEpwJ_3nfwJHBxw

D. CHALLENGES

There is significant growth and potential in building an inclusive digital infrastructure across SARFII countries. However, a major concern remains the wide gender gap in financial access and limited digital finance literacy, particularly among older, female, rural, and disabled populations, groups that are more vulnerable to cyberattacks. Inadequate regulatory coordination across sectors also leads to disjointed incident response efforts, complicating the effective management of large-scale cyber threats.

Building trust, confidence, and safety requires a targeted approach involving strong regulatory frameworks, enhanced consumer education, and technology-driven fraud prevention. Some member countries have successfully increased digital payment adoption and literacy by deploying local ambassadors (such as community leaders, municipal employees, or social service workers) and digital account agents who engage directly with users, especially women and vulnerable groups, to promote equitable participation in the digital economy. Lastly, more tailored policies and guidelines are needed to support persons with disabilities who may lack equal access to financial services. Regional examples include voice-guided and soundbox-enabled services for the visually impaired.

E. ACCESS TO SME AND MSME FINANCE

MSMEs play a critical role in economic activity and are key drivers of growth. Expanding their access to affordable, sustainable financial services is crucial for inclusive development, with far-reaching benefits for the broader economy. Across the region, digital finance is beginning to transform SME lending and promote financial inclusion. Government-backed credit guarantees, such as Pakistan's Risk Coverage Scheme for SMEs, which offer 20 percent portfolio-based risk cover for small enterprises and 10 percent for medium enterprises,[36] have eased some hurdles, though challenges remain that must be addressed to fully harness the potential of digital finance in empowering SMEs.

I. GAPS IN SME ACCESS TO FINANCE

Many SMEs struggle to access credit due to traditional lending models that rely on collateral and formal business records. According to a 2025 IFC report, Indian SMEs represent 68 percent of the region's USD333 billion SME finance gap.[37] In Pakistan, credit to SMEs declined further during COVID-19, dropping from 7.6 percent in December 2019 to 6.5 percent by December 2021.[38] Nepal has seen rising SME loan volumes, yet the World Bank estimated a USD3.6 billion financing gap in 2020, which represents roughly 10 percent of its GDP.[39]

Women-led SMEs face even greater barriers. In Bangladesh, the financing gap in this segment stands at USD2.8 billion, "where 60 percent of women SME's financing needs are unmet."[40] A study by ADBI and Cambridge[41] found that while men had a marginally higher success rate in securing bank funding compared to women (55 percent versus 58 percent), women outperformed men in obtaining microfinance funding (88 percent versus 59 percent). Given that women are more likely to run smaller enterprises, with 81 percent reporting as sole traders or micro business owners compared to 66 percent of men,[42] there is a clear need to scale digital microfinance solutions tailored to their needs.

While digital lending platforms are emerging in countries such as Nepal and Pakistan, their impact is limited by fragmented credit data and outdated lending practices. Without reliable digital records, many SMEs, especially those in rural areas, remain underserved, as Licensed Financial Institutions (LFIs) are unable to assess their creditworthiness, leading to higher interest rates and restricted funding. In contrast, platforms like LendingKart and Kinara in India leverage alternative data from digital transaction histories to expand access, which could provide a more inclusive solution with robust regulatory support.

II. BRIDGING THE URBAN-RURAL DIVIDE

Rural and vulnerable communities often remain underserved, as limited digital literacy and infrastructural gaps continue to hinder the adoption of digital financial services. Language barriers also pose a challenge, since most LFIs and FinTechs tend to offer services in English or just one language when it comes to mobile services, while multilingual support is more common in online banking platforms. Policy initiatives are therefore needed to promote the delivery of mobile DFS in multilingual languages to ensure accessibility for all users.

36 As noted by the State Bank of Pakistan.

37 International Finance Corporation. 2024. Small Business, Big Impact: Empowering Women SMEs for Success. Available at: https://www.ifc.org/en/stories/2024/small-business-big-impact

38 SME Finance Forum. 2025. MSME Finance Gap. Available at: https://www.smefinanceforum.org/sites/default/files/Data%20Sites%20downloads/IFC%20Report_Annex%20ONLY%20Final%203%2025.pdf

39 World Bank. 2024. Project Information Document (PID). Available at: https://documents1.worldbank.org/curated/en/099122124190031063/pdf/P508961153e9470619ef7162eecad985c9.pdf

40 World Bank. n.d. Small and Medium Enterprises (SMEs) Finance. Available at: https://www.worldbank.org/en/topic/smefinance

41 Available at: https://vayana.com/wp-content/uploads/2025/01/2025-msme-access-to-digital-finance-study-emde-asia.pdf

42 Id.

CASE STUDY: Sri Lanka's Digital Literacy Programs and Financial Inclusion Surveys

Sri Lanka, with an adult literacy rate at over 92 percent,[43] presents a unique case in digital financial literacy. Despite strong educational indicators, digital adoption gaps persist, especially among rural, elderly, and female populations. The Central Bank of Sri Lanka (CBSL) leads financial inclusion and digital literacy efforts through its NFIS, which focuses on digital finance, MSME finance, consumer protection, and financial literacy. The strategy features widespread media outreach across TV, radio, print, and social media emphasizing fraud prevention, digital onboarding, QR payments, and broader use of digital payments. CBSL delivers over 400 educational programs annually through its six regional offices, along with financial literacy and entrepreneurship lessons in schools (from Grade 6) and technical colleges. Targeted efforts support underserved groups, including women, using midwives as literacy messengers and sessions on gender-specific banking, scam awareness, unauthorized lenders, and digital onboarding.

The National Financial Inclusion Surveys, conducted periodically with partners such as the National Payment Council, NGOs and the private sector, are a key way to evaluate digital literacy and DFS adoption using demand-side data, stakeholder feedback, and gender disaggregated insights. Complementary financial literacy surveys measure consumer knowledge and attitudes, while CBSL leverages payment system, institutional, and regional data to monitor account ownership, DFS, and app usage at a granular level.

CBSL evaluates the impact of its initiatives through OECD-based surveys, stakeholder feedback, grassroots assessments, and compliance and consumer satisfaction surveys. These reveal a range of insights, including gender disparities in digital payment use, dependence on informal borrowing, low trust in formal systems, and vulnerability to scams among rural and underserved groups. They also highlight challenges which elderly and low digital literacy users face with smartphones, multiple apps, and unfamiliar digital systems, amid rising threats like pyramid schemes, OTP scams, and online fraud.
Sri Lanka's approach offers a scalable model for countries with similar socioeconomic contexts, demonstrating how integrated stakeholder collaboration and targeted outreach to women and rural communities can bridge the digital divide. Its continuous measurement and feedback mechanisms also underscore the importance of behavioral change in translating knowledge into meaningful adoption.

David Keith Brown / Alamy Stock Photo

43 Further information is available at: https://data.worldbank.org/indicator/SE.ADT.LITR.ZS?name_desc=true

There is growing recognition that innovation in financial products can drive inclusion. These range from QR-based merchant payments to real-time digital remittances by citizens living abroad. Open Banking and integration with e-commerce can further expand access to digital financial services. Lending remains crucial to both consumer and SME economies, and across the region, LFIs are beginning to deploy digital lending solutions tailored to the needs of SMEs, enabling faster and more efficient credit assessments. However, the full potential of these innovations is still untapped. FIs are still transitioning from traditional, paper-based credit evaluations to streamlined, digital processes for real-time risk assessment. In parallel, stronger policies and frameworks are needed to support Open Finance, cross-border payments, and the adoption of updated technical standards.

F. LEGAL AND REGULATORY FRAMEWORKS

A well-structured legal and regulatory framework is vital for the stability and growth of the digital finance ecosystem. Across the region, efforts are underway to update legal systems and regulations to keep pace with new business models, rapid FinTech innovations and DFS, aiming to promote trust, innovation, and inclusiveness.

Sri Lanka and Pakistan, for instance, are modernizing their digital finance laws to balance innovation with consumer protection. Sri Lanka amended its Electronic Transactions Act No. 19 of 2006 to align with the United Nations Electronic Communications Convention, enhancing the legal validity of electronic communications and contracts, facilitating cross-border trade, and promoting paperless transactions.[44] The law now supports electronic signatures and biometric authentication, enhancing trust and efficiency in DFS. Additionally, Sri Lanka's 2025 budget proposes launching a Digital Economic Authority to regulate and supervise the evolving digital sector.[45] Pakistan's Securities and Exchange Commission amended the Non-Banking Finance Companies (NBFC) regulations to accommodate new technologies,[46] while Visa's 2024 strategic partnership with 1Link aims to expand digital payment infrastructure and significantly increase the number of businesses accepting digital payments nationwide.[47]

Concurrently, Nepal and Bhutan are updating their regulatory frameworks to reflect FinTech's growing influence, including comprehensive cybersecurity guidelines and rules for digital-only bank licenses, similar to Pakistan which issued licenses to five digital-only and full-service digital banks in 2023.[48] The NRB implemented 'Cyber Resilience Guidelines' in August 2023,[49] mandating banks and financial institutions to develop cyber resilience strategies, conduct risk assessments, implement ISO 27001-aligned security controls, and establish continuous monitoring and incident response plans. Bhutan's National Digital Identity Act, also passed in 2023, marking a key milestone in facilitating digital interactions between citizens and public or private institutions and stakeholders.[50]

While these reforms reflect a strong commitment to creating a regulatory environment that balances innovation with risk mitigation, regulatory fragmentation remains a serious obstacle to digital transformation. Diverse legal structures and overlapping mandates across the banking, insurance, and securities sectors create uncertainty for FIs and FinTechs, and coupled with outdated legal provisions, often result in inconsistent enforcement and compliance challenges. Many regulatory provisions have not kept up with evolving digital business models, making it difficult for new entrants to navigate the market. Additional hurdles stem from outdated civil and criminal laws, such as requirements in some jurisdictions for court orders to freeze suspicious accounts. Frictions also arise from inconsistencies across provincial and cross-border legal systems, further slowing progress.

44 Electronic Transations Act 2006 (Sri Lanka). Available at: https://lankalaw.net/2024/03/11/electronic-transactions-act-2006/

45 Lanka News Web. 2025. SL Government to Introduce Digital Currency in Economic Modernization. Available at: https://lankanewsweb.net/archives/69763/sl-government-to-introduce-digital-currency-in-economic-modernization/

46 Securities and Exchange Commission of Pakistan. n.d. SECP Amends NBFC Regulations to Adapt to New Technologies. Available at: https://www.secp.gov.pk/media-center/press-releases/secp-amends-nbfc-regulations-to-adapt-to-new-technologies/?utm_source=chatgpt.com

47 Reuters. 2024. Visa aims for 10-fold rise in Pakistani use of digital payments. Available at: https://www.reuters.com/business/finance/visa-aims-10-fold-rise-pakistani-use-digital-payments-2024-09-11/?utm_source=chatgpt.com

48 State Bank of Pakistan. 2023. SBP Awards In-principle Approval to Five Proposed Digital Retail Banks. Available at: https://www.sbp.org.pk/press/2023/Pr-20-Sep-2023.pdf

49 Fiscal Nepal. 2024. Central bank strengthens cyber resilience guidelines amid rising cybercrime concerns. Available at: https://www.fiscalnepal.com/2024/02/19/15663/central-bank-strengthens-cyber-resilience-guidelines-amid-rising-cybercrime-concerns/

50 GovTech Bhutan, ESCAP, and UNDP. 2023. Kingdom of Bhutan Digital Economy Development and Transformation Strategy. Available at: https://www.undp.org/sites/g/files/zskgke326/files/2024-05/UNDP_Bhutan%20Digital%20Development%20and%20Transformation%20Strategy.pdf#page=23.67

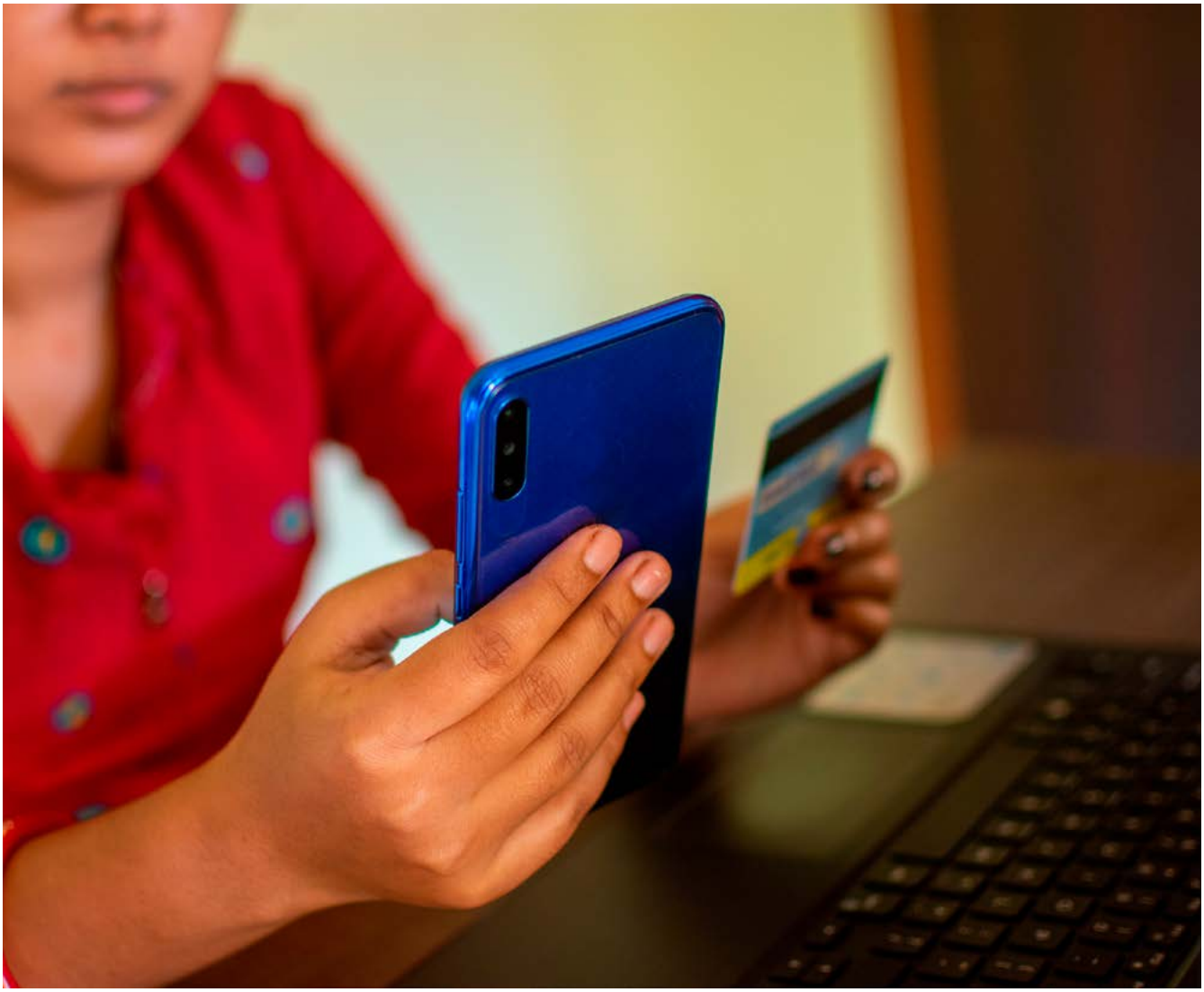
Maskot / Alamy Stock Photo

3. INCLUSIVE DIGITAL INFRASTRUCTURE: BENCHMARKS FOR THE NEXT LEVEL OF INCLUSIVE GROWTH AND DEVELOPMENT

In developing recommendations for the next generation of inclusive digital finance, FT4FI and IDI examined a range of possible benchmarks to guide implementation over the next three to five years across SARFII. These are summarized below by key project themes.

A core reference is AFI's 2018 Strategy on the Role of Technology in Financial Inclusion, reaffirmed in the Sochi Declaration. The FT4FI strategy was based on a decade-long global review of the use of technology in financial inclusion and centered on four pillars. These would now be described as elements focused on IDI (including digital ID), interoperable payments systems, simplified account opening, eKYC, government-to-person digital payments, GovTech, and various forms of traditional financial infrastructure including securities infrastructure and credit, or other information registries. This strategy was subsequently expanded in a series of AFI publications which included regulatory strategies and ecosystem development.

Building on this foundation, the team also reviewed international ID experiences, including engagement with a range of stakeholders in India to assess early implementations and identify emerging priorities for IDI development.



Somnath Mahata / Shutterstock

CASE STUDY: India's Experience with Digital Public Infrastructure (DPI)

India's digital financial transformation has been driven by the India Stack[51] strategy, built on a set of interlinked digital infrastructures. At its core is Aadhar, a biometric digital ID now covering 95 percent of the population. Aadhaar has enabled the majority of the population, which lacked formal government-issued identity documents, to join the formal and the digital economy, accelerating access to digital services, especially DFI. The Reserve Bank of India (RBI) supported this transformation with updated digital finance regulations, tailored FinTech rules, and the creation of a Payments Bank framework. It also launched Self-Regulatory Organization (SRO) and Account Aggregator (AA) frameworks to address new DFS segments, alongside the Payments Infrastructure Development Fund (PIDF)[52] to subsidize payment infrastructure in smaller centers.

India's Digital Public Infrastructure (DPI) projects, notably the UPI,[53] have played a central role. UPI, now the world's largest real-time payments network, handles over 600 million transactions daily with a low fraud rate. In March 2025 alone, it recorded INR24.77 trillion (about USD300 billion) in transactions, driven by increased digital payment adoption during COVID-19 and a doubling in internet users[54] due to affordable mobile data.

51 Further information is available at: https://indiastack.org/index.html

52 Further information is available at: https://rbi.org.in/scripts/FS_Notification.aspx?Id=12009&fn=9&Mode=0

53 Further information is available at: https://www.npci.org.in/what-we-do/upi/product-statistics

54 Further information is available at: https://www.statista.com/statistics/792074/india-internet-penetration-rate/

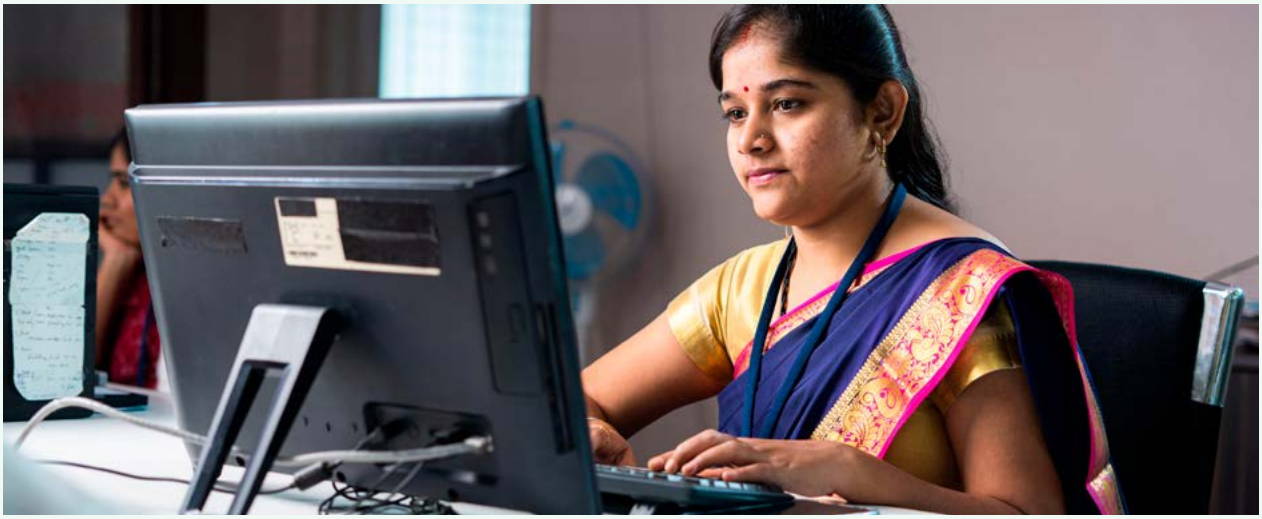
The AA framework has also scaled rapidly, enabling consent-based data sharing that improves credit access and financial planning. As of February 2025, it has supported over 130 million accounts and 160 million successful consents.[55] By integrating with Aadhar, UPI, DigiLocker, and other layers, it has helped lenders operate more efficiently, disbursing INR426 billion [56] in unsecured loans in just six months.

Key barriers persist despite strong progress, including the urban-rural digital divide, limited digital access for some groups, and gaps in DFS availability in local languages. Although smartphone penetration is rising, USSD options remain vital for feature phone users and the elderly. Solutions for vulnerable groups, such as sound-based solutions for the hearing impaired, are also needed. Finally, while mobile payments have scaled impressively, many transaction fees and MDRs have been waived or discounted.[57] Policymakers, in collaboration with the Ministry of Finance, NPCI, and the industry, must explore sustainable models focused on long-term viability. These challenges highlight the need to assess first-generation IDI and FT4FI approaches and advance second-generation strategies going forward.

55 Further information is available at: https://sahamati.org.in/aa-dashboard/

56 Sahamati. 2024. Account Aggregator Ecosystem: Transforming India's Financial Services. Available at: https://sahamati.org.in/wp-content/uploads/2025/01/Account-Aggregator-Adoption-update-31st-Dec-2024.pdf

57 Ministry of Finance (India). 2025. Advancing Cashless India - ₹1,500 Cr Incentive Scheme for Low-Value BHIM-UPI Transactions. Available at:https://pib.gov.in/PressReleasePage.aspx?PRID=2114335#:~:text=Since%20January%202020%2C%20to%20promote,Income%2Dtax%20Act%2C%201961



Lakshmiprasad S / Alamy Stock Photo

Building on experiential reviews conducted by organizations such as the World Bank, World Economic Forum, and G20, the team synthesized key focus areas to inform and guide a broader IDI strategy, summarized below.

A. INCLUSIVE DIGITAL INFRASTRUCTURE

I. FOUNDATIONS: FIRST-GENERATION IDI

At the core of first-generation IDI, as detailed in the AFI Sochi Declaration and FT4FI Strategy, are foundational elements now reframed to reflect a decade of experience. Digital inclusion, particularly mobile and internet access, is the starting point for digital transformation. For second-generation strategies, assessing penetration levels and barriers, such as high data costs and weak infrastructure, is essential to understanding both progress and key roadblocks. Mobile technology remains critical, but access alone is not enough. Addressing affordability, barriers to access, and infrastructure quality, especially in rural areas, is key to bridging the digital divide.

Interoperable electronic payments are another central pillar, underpinned by national RTGS and FPS systems along with supportive regulations. These enable near real-time transactions between different FSPs, often through a central switch. In some cases, regulatory mandates can ensure broader participation, encouraging a level playing field. Interoperability reduces friction in payments, promotes competition, and is a vital building block for other DFS.

The second core element is identity, reflected in the form of a national digital ID system, usable across financial and government services. A secure, widely accepted digital ID system streamlines user authentication, increases efficiency, and improves access to essential services for all citizens. With the core IDI ID system in place, second-generation strategies must focus on adoption and usability to unlock its full benefits.

Access to a financial or mobile money account or digital wallet links digital and financial inclusion. First-generation IDI strategies aim for high, ideally universal, account access to ensure that a large proportion of the population has a gateway to participate in the digital economy, including the most marginalized individuals. Increased account and mobile money usage enables savings, payments, and access to other financial products and services. Success relies on eKYC systems and the availability of government payment systems.

An effective eKYC system is essential to first-generation IDI strategies, simplifying account opening while adhering to regulatory requirements. Traditional KYC procedures can be cumbersome and time-consuming, limiting access to financial inclusion. By enabling remote, digital identity verification, eKYC is able to lower costs, improve customer experience, and expands access to formal financial services, particularly in remote areas.

II. MOBILIZATION OF FINANCE

Experience with FT4FI and IDI strategies shows strong potential to advance financial inclusion. However, reviews highlight that while first-generation IDI is necessary, it is insufficient, as true inclusion requires not just account access but meaningful use of financial services that drive inclusive, sustainable development. Mobilization is therefore central to a second-generation IDI strategy.

EGovPayments play a critical role in the mobilization of digital transformation, though more must be done beyond effective implementation. Success requires more than getting systems up and running, it depends on continuous improvement and alignment with other IDI components and the broader DFS ecosystem. Seamless integration can improve efficiency, reduce redundancies, and create a more unified digital payments landscape for both government and citizens.

III. NEXT STAGE OF DEVELOPMENT: BUILDING SECOND-GENERATION IDI STRATEGIES

Second-generation IDI strategies are evolving to address emerging needs, including advanced systems for fraud prevention and consumer protection, data mobilization within Open Banking and Open Finance frameworks, support for AI, foundational systems for credit data, and innovations in digital finance such as central bank digital currencies (CBDCs), tokenization, and other digital assets.

As digital and financial inclusion expand, so do the risks, especially the growing scale of digital crime. Building on first-generation IDI frameworks, digital ID, and mobile access, countries are now developing integrated fraud and consumer protection mechanisms, including IDI, as part of their core infrastructure. These systems are essential for detecting and preventing abuse while also building user trust, ensuring transparency, providing effective grievance redress, and promoting informed consumer participation – all of which are vital for the sustainable growth and widespread adoption of digital financial ecosystems.

Megapress / Alamy Stock Photo

As countries explore the future of digital finance, building capacity around CBDCs and virtual assets becomes increasingly important. Several central banks in the region, including in India, Nepal, and Bhutan, are running pilots or considering near-term launches. Effective implementation will not only require the right technical expertise but also a strong understanding of the potential benefits, risks, and design choices, including whether to issue wholesale or retail CBDCs and how to integrate them with existing systems while managing monetary policy implications. For non-CBDC virtual assets, a key consideration for capacity building lies in meeting Anti-Money Laundering (AML) monitoring requirements. Any regulatory or operational framework for CBDCs or virtual assets must embed effective safeguards to prevent illicit financial flows and protect the integrity of the financial system.

B. CYBERSECURITY

Digital and financial inclusion through first-generation IDI and FT4FI strategies have also introduced new digital risks, requiring well-designed frameworks to address emerging cyber threats from the perspective of consumer protection but also in terms of financial stability and national security. A key priority is establishing a comprehensive cybersecurity reporting and information-sharing framework that extends beyond traditional banks to include all financial institutions, including non-bank financial service providers and FinTech companies, as they become increasingly interconnected. Such systems enable early threat detection, coordinated responses, and collective resilience.

Equally important is the implementation of mandatory internal cybersecurity controls within financial institutions, supported by effective regulatory supervision. These controls should cover access management, data protection, and incident response, while regular audits can help identify vulnerabilities and ensure ongoing improvement. In addition, financial institutions must maintain robust continuity plans to guide their response during cyber incidents or system outages.

A dedicated Chief Information Security Officer (CISO) function and strong cyber security systems within the central bank or designated regulatory agency are essential for coordinating sector-wide efforts. These institutions play a critical role in setting standards, providing guidance, and monitoring compliance across the industry. A strong in-house cybersecurity capability is necessary for effective oversight and response to emerging threats.

Beyond national efforts, there is potential for increased regional cooperation through the development of a cybersecurity information-sharing framework. Given the cross-border nature of cyber threats, this kind of collaboration can significantly enhance collective defenses by enabling timely exchanges of threat intelligence, early warnings, and coordinated responses to incidents with regional implications. This approach supports a more resilient digital financial ecosystem across the region.

C. CONSUMER PROTECTION

As digital and financial inclusion expand, they introduce new risks that require rapid responses to maintain confidence in the financial system while protecting the most vulnerable from predatory practices. A strong foundation lies in developing comprehensive consumer protection strategies supported by IDI, which must address the unique risks of the digital environment, such as data privacy breaches, fraud, and unfair business conduct, while also accommodating the diverse needs and varying levels of digital literacy across populations.

This protection should go hand in hand with efforts to improve financial and digital literacy. Regulatory safeguards and education initiatives must work together to equip users to make informed decisions while confidently managing digital risks. As DFS evolves, continued investment in literacy is crucial to ensure inclusive and safe participation. Similarly, there is a clear need for consistent data collection metrics, nationally and ideally across regions or globally, potentially led by networks like AFI in coordination with major financial inclusion and development partners.

D. DIGITAL AND FINANCIAL LITERACY

While IDI and FT4FI strategies can be transformative, they need to be reinforced with broader measures to deliver lasting impact. Advancing to the next stage and maximizing the impact of first-generation IDI strategies requires a sustained focus on digital and financial literacy, though the process is far from simple. The first step is developing a national digital and financial literacy strategy, which should define clear objectives, target specific population segments, and identify key initiatives to build essential knowledge and skills in digital technologies and financial management.

Equally important is the creation of an effective monitoring and assessment framework. Measuring literacy programs calls for regular tracking tools, including return on investment assessments and voice of the customer (VOC) surveys to capture satisfaction, user experience, and perceptions. These tools help evaluate progress, identify areas for improvement, and ensure that interventions adapt and deliver. Under the SARFI framework, AFI could assist members in adopting these tools and in benchmarking service quality, enabling countries to build more responsive and inclusive literacy ecosystems.

E. LAW AND REGULATION

Developing legal and regulatory frameworks is central to the success of first-generation IDI and FT4FI strategies. Advancing to the next level requires both consolidation and addressing emerging issues, particularly in relation to data law and regulation.

At the foundational level, continuous updates to payments laws and regulations are essential to keep pace with evolving technologies and business models. This includes revising legal frameworks and supervising new payment service providers, regulating digital instruments, and strengthening consumer protection in digital payments. As DFS expands, regulation of non-bank financial institutions also needs to evolve, which requires developing tailored frameworks that address risk, consumer protection, and systemic stability.

A key feature of the next level IDI strategies is robust data governance. With increasing data usage on digital platforms, comprehensive data protection laws must set clear rules for collection, processing, storage, and sharing, while safeguarding individual rights. Strong data regulation and supporting infrastructure are vital to build trust and ensure security in the digital economy.

4. MAJOR ACTION RECOMMENDATIONS: MEDIUM-TERM (THREE TO FIVE YEARS) – BUILDING THE CAPACITY OF REGULATORS, INDUSTRY, AND CONSUMERS

Drawing on the current status (Section II) and best practice benchmarks (Section III), this section outlines key recommendations for SARFII members over the next three to five years. Strengthening the capacity of regulators, industry, and consumers will be central to maximize the impact of first-generation IDI and advance second-generation IDI strategies.

A. ENHANCING REGULATORY CAPABILITIES

Over the past decade, technology in financial services has evolved rapidly and at scale. Regulators must not only oversee traditional LFIs but also strengthen their ability to manage emerging opportunities and risks. Investing in staff capacity, upskilling, and equipping them with the right tools and processes will be vital across the region.

I. ENHANCED LICENSING AND OVERSIGHT PROCESSES

Strengthening licensing processes for digital-only banks and FinTechs is essential to enhance the ability of central banks to supervise digital financial services models. Streamlined procedures should be established to facilitate fast and secure market entry, enabling new players to innovate without compromising regulatory standards. This modernization should also include the adoption of advanced RegTech and SupTech solutions to support real-time compliance monitoring, risk management, and continuous oversight, ensuring that regulatory practices keep up with technological advancements.

II. FLEXIBLE REGULATORY APPROACHES

Regulators are encouraged to adopt innovative and flexible frameworks that allow for “test and learn” environments, enabling LFIs and FinTechs to innovate while enhancing regulatory understanding of these new business models. For example, by establishing dedicated regulatory sandboxes that address crucial policy issues related to emerging digital finance business models, policymakers can provide controlled environments where FinTechs and licensed entities can pilot new technologies such as QR-based payments and instant transfer systems, without compromising consumer protection or systemic stability.

Pikselstock / Alamy Stock Phot

III. FORMATION OF FINTECH INNOVATION HUBS

In addition to regulatory sandboxes, creating dedicated FinTech and innovation teams or hubs can both catalyze ecosystem growth and increase regulatory technical capability. These hubs help design frameworks for DFS innovation, conduct proof-of-concept (POC) projects, and promote relationships among stakeholders, including financial institutions, startups, and technology providers. Their role is to bridge gaps between traditional financial services with emerging digital solutions while providing market intelligence on the effectiveness of DFS regulatory frameworks.

A notable example is the RBI's Innovation Hub (RBIH)[58] established in 2021 to promote inclusive access to financial services through cutting-edge technology. RBIH operates on two main fronts: developing innovative tools, such as the MuleHunter tool, and driving broader innovation in the ecosystem through initiatives like tech sprints, hackathons, and bootcamps under the FinTech and Startup Acceleration (FAST) initiative. FAST consists of masterclasses, mentorships, market access, investor engagement, and mixers that bring together regulators, enablers, and innovators to strengthen the ecosystem.

IV. BUILDING COLLABORATIVE FRAMEWORKS FOR CYBER THREATS

Cyber threats are often cross-agency and multi-faceted, requiring urgent but coordinated responses. Establishing inter-agency councils that include regulators, FIs, law enforcement, and cybersecurity experts can facilitate real-time threat intelligence sharing and enable unified, timely responses to emerging threats. A relevant example is Malaysia's Jangan Kena Scam campaign. Launched by the Association of Banks in Malaysia and the Association of Islamic Banking and Financial Institutions Malaysia, and supported by Bank Negara Malaysia (BNM),[59] this initiative aims to raise public awareness, educate citizens on how to identify scams, and equip them with practical tools for self-protection.

V. INTER-AGENCY COLLABORATION

Effective regulation in the digital era requires coordinated efforts across national and provincial regulatory bodies, enabling them to leverage shared knowledge and resources. Establishing inter-agency councils or dedicated coordination committees will promote continuous dialogue among regulators, FIs, and technology providers, ensuring that emerging challenges such as cybersecurity threats or rapid technological changes are addressed proactively through joint initiatives and shared best practices.

58 Further information is available at: https://rbihub.in/

59 Further information is available at: https://www.jangankenascam.com/

B. DEVELOPING INDUSTRY CAPABILITIES

From an industry standpoint, IDI can provide mechanisms to unlock new business models that support inclusive sustainable development while reducing the costs of customer acquisition and credit evaluation. The following are several priority areas for action:

I. ENHANCED VERIFICATION CAPABILITIES

Upgrading ID verification processes is critical, particularly through advanced biometric methods, including app-based authentication. A tiered approach, offering basic account services with minimal onboarding and more comprehensive features requiring higher levels of verification, can balance convenience, inclusion and security. This allows consumers to easily access low-value transactions while safeguarding sensitive and large-sized financial transactions.

II. ESTABLISHING DIGITAL SME IDENTIFIERS

A digital SME ID would serve as a game-changer for accessing a wide range of financial services by streamlining processes for account opening, credit evaluation, and loan disbursement. A unified identifier would standardize business performance assessment and link transactional data directly to credit scoring, offering a more dynamic and accurate reflection of an SME's financial health.

III. DEVELOPING UNIFIED DATA PLATFORMS

To maximize the benefits of high-speed connectivity, secure unified data platforms are needed to support real-time analytics and regulatory reporting. Standardized data integration across financial institutions will enhance monitoring, enable quicker decision-making, and accelerate innovation cycles. These platforms can harness big data to optimize transactions and drive targeted policy interventions aligned with sustainable development goals.

IV. DIGITALIZING CREDIT ASSESSMENTS AND LENDING

Traditional lending models often rely heavily on collateral and formal credit histories, excluding many SMEs from much-needed financing, particularly those in rural or underserved markets. The adoption of digital lending platforms that leverage alternative data sources, such as transactional histories, mobile payment records, and other digital footprints, can improve credit assessments and broaden access. Coupled with digital supply chain financing, this approach can bring increased operational efficiency to SME lending while scaling up transaction volumes and strengthening risk management and compliance practices.

V. ENHANCED CYBERSECURITY AUDITS AND CYBER RESILIENCE

While regular audits and penetration tests remain essential to identify IT vulnerabilities, audit processes and assessment scopes must be streamlined to provide clear industry guidance and readiness. Establishing a routine schedule, baseline auditor requirements, along with real-time monitoring and incident response drills will help ensure that security measures remain effective and adaptable to emerging threats.

Beyond immediate threat detection and response, organizations must also invest in long-term cyber resilience, which encompasses strategic planning for operational continuity, data recovery, and business continuity in the event of major cyber incidents. Strengthening resilience ensures that both technological systems and organizational processes can effectively adapt to and recover from disruptions.

VI.STREAMLINING LENDING PROCESSES

Simplifying the lending process is critical to expanding access to credit for SMEs and underserved consumers. This involves reducing bureaucratic hurdles and adopting technology-driven solutions to accelerate loan approvals. By integrating centralized credit registries and digital identity verification systems, FIs can reduce paperwork, shorten turnaround times, and ultimately provide SMEs with faster access to capital, thereby increasing the credit capacity of SMEs and their wider ecosystems.

VII. ENHANCING GOVERNMENT PAYMENT DIGITALIZATION

Accelerating the digitalization of government payments and receipts across all departments is another key element that can build stronger financial infrastructure. While many governments have begun adopting digital payments, implementation often remains limited to specific use cases or sectors. A more integrated approach linking various government departments through a universal payments framework that includes faster payment systems, online banking, and mobile money, can improve efficiency, transparency, and convenience. This not only simplifies transactions for citizens and lowers costs, but also provides governments with real-time data for better decision-making and targeted service delivery.

The following table presents an overview of G2P payments across the region:

Country	Key Platforms	Examples
Bangladesh	Electronic Fund, Transfer Network, Mobile Money Accounts	Social Safety Net Payments
Pakistan	BISP, Branchless Banking	Benazir Income Support Programme
Sri Lanka	Sri Lanka Interbank Payment System (SLIPS)	Social Security Allowances
Nepal	Connect IPS	Social Security Allowances
Bhutan	Digital NID Linked Accounts	Social Welfare Disbursements
Maldives	eFaas Linked Mobile Payments	Pension and Subsidy Payments

CASE STUDY: Sri Lanka GovPay

Launched in February 2025, GovPay[60] is a collaborative effort by Sri Lanka's Information and Communication Technology Agency (ICTA) and LankaPay Payments and Product Strategy Advisor, guided by the CBSL and supported by the Ministry of Digital Economy. The platform enables citizens and businesses to make secure, real-time payments to government institutions, reducing the need for physical visits, improving transparency, and minimizing cash dependency. GovPay offers a single, easy-to-use digital interface for government-related payments and supports transactions via internet banking portals as well as any mobile banking or payment apps. Its goals include boosting real-time fund transfers to the government and increasing transaction transparency by eliminating manual errors, fraud, and cash handling. Furthermore, GovPay strengthens financial reporting and auditing processes while reducing administrative overhead through automated payments.

Built on the Instant Payment System (CEFTS infrastructure) and the LankaPay Online Payment Platform (LPOPP), GovPay enables real-time reconciliation of payer records within government institutions and allows institutions without digitalized databases to benefit from instant payment receipts and day-end record reconciliation. Users can pay for a range of services, including taxes, utility bills, fines, and educational fees. The platform facilitates instant account-based P2G transfers initiated via internet banking or payment apps. Real-time processing ensures that users receive instant SMS or email confirmations from both their bank and the relevant government agency. At launch, GovPay connected 16 government institutions, with plans to expand to 46 by April 2025.[61] Key participants include the Department of Ayurveda, Sri Lanka Port Authority, Telecommunications Regulatory Commission, University of Colombo, State Timber Corporation, and various Divisional Secretariats and Local Councils.

Challenges include digital literacy gaps in remote areas and ensuring smooth onboarding and integration of all government entities. Some departments may require investments to upgrade limited digital infrastructure and processes. In the coming months, GovPay will provide multi-language support and simplified interfaces to improve the user experience. By streamlining government financial transactions, enhancing service delivery, and encouraging digital payments, this platform strengthens both citizen engagement and public sector efficiency.

60 Further information is available at: https://govpay.lk/

61 Further information is available at: https://govpay.lk/what-is-govpay/

VIII. DEVELOPMENT AND PROMOTION OF INDUSTRY ASSOCIATIONS

Supporting the development of FinTech associations can help lay a structured foundation for sector growth. In member countries with no formal representative bodies, regulators should consider supporting the creation of segment-based associations focused on key DFS verticals, such as payments and digital lending. These associations serve as critical bridges between the regulators and industry, providing platforms for organized feedback, regulatory consultation, and ecosystem development. In countries where these associations do exist, regulators should formalize engagement and actively involve them in consultations on new and updated regulations to ensure industry perspectives inform policy design.

Industry associations can also serve as launchpads for SROs, especially in areas involving emerging business models such as digital lending, account aggregation, and virtual assets, as highlighted by India's RBI, which introduced the SRO-FT[62] framework to promote responsible innovation in the FinTech sector. Under this model, SROs are industry-led bodies that establish and enforce regulatory standards, promote ethical conduct, safeguard market integrity, resolve disputes, and encourage transparency and accountability among its members. Similarly, Japan's FSA established an SRO for virtual asset service providers in 2018, before the development of a formal regulatory framework.[63]

62 Reserve Bank of India. 2024. Framework for Self-Regulatory Organisation(s) in the FinTech Sector. Available at: https://rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1263

63 Baker McKenzie. 2018. Japanese Financial Services Agency accredits the Japan Virtual Currency Exchange Association as a Self-Regulatory Organization. Available at: https://blockchain.bakermckenzie.com/2018/11/13/japanese-financial-services-agency-accredits-the-japan-virtual-currency-exchange-association-as-a-self-regulatory-organization/

These associations also serve as platforms for joint financial literacy initiatives between regulators and FinTechs and help foreign firms navigate local markets by offering insights, guidance, and regulatory connections through their member networks.

C. END USER ENABLEMENT

Beyond regulator and industry support, IDI can also play an important role in advancing financial inclusion, especially for last mile and excluded groups.

I. BRIDGING THE URBAN-RURAL DIGITAL DIVIDE

While urban areas continue to benefit from high digital adoption, rural regions face significant challenges due to low digital literacy and limited connectivity. Deploying mobile-based and offline verification tools can help bridge this gap by enabling access to DFS without the need for constant internet access.

Expanding branchless banking, mobile payment accounts, and agent networks can be a major catalyst in extending DFS beyond urban centers, especially in underserved areas. Interoperability of branchless banking agents, similar to the pilot being run in Pakistan, can further enhance this reach.[64] Mobile banking units, local agent support, and tailored financial products can narrow the urban-rural financial access divide.

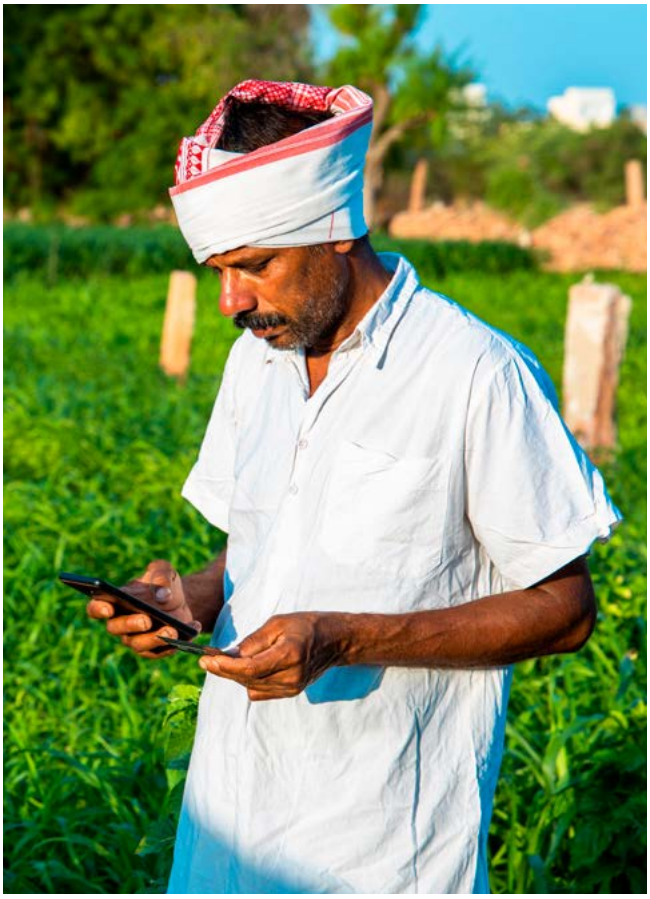
II. RISK-BASED DEPLOYMENT OF USSD SOLUTIONS

Since not all users have smartphone or high-speed internet access, USSD-based solutions remain an essential, cost-effective tool to reach a wider audience, particularly in rural areas. Reviewing the effectiveness of existing USSD frameworks and adopting a risk-based approach when updating these solutions can help address safety and consumer protection concerns while supporting broader access to DFS.

III. LEVERAGING GOVERNMENT AND COMMUNITY INITIATIVES

Collaboration with government programs is crucial to enhance outreach. For example, by integrating digital identity initiatives with existing rural development schemes, policymakers can boost account onboarding and drive digital literacy. Establishing community-based training programs and local support centers will educate citizens on using digital identity tools and help them understand the benefits and security measures in place.

64 As noted by the State Bank of Pakistan.



Gajendra Bhati / Alamy Stock Photo

IV. TAILORED OUTREACH PROGRAMS

Subsidized mobile connectivity and localized digital literacy campaigns can empower underserved populations to fully engage in the digital economy. Alongside regulatory reforms, investing in consumer education is vital to promote safe digital practices, emphasize cybersecurity, and ensure consumers understand their rights in the digital financial landscape. Special attention is needed for vulnerable groups, including women, minorities, the elderly, rural communities, and economically disadvantaged populations. Tailored initiatives can include subsidized mobile connectivity, localized financial education, and credit products designed for these communities.

V. ONGOING TRAINING AND CAPACITY BUILDING

Financial institutions and regulators should work together to organize regular training sessions, workshops, and public campaigns. Additionally, ongoing investments in cybersecurity awareness and digital literacy is vital to support digitalization across member countries. These efforts should be ongoing, as increasing digital adoption will amplify exposure to cyber risks and threats.

CASE STUDY: Bhutan's Digital Drukyul

Bhutan's Digital Drukyul Flagship Program was launched under the 12th Five-Year Plan (2018-2023) to modernize government services, improve digital literacy, and ensure equitable access to technology nationwide. Since its inception, the program has rolled an Education Information Management System, Electronic Patient Information System, Integrated Taxation System, and most notably, the National Digital Identity (NDI) launched in 2023. The NDI provides citizens with a unique digital identity facilitating secure online authentication and transactions. Importantly, the system does not collect or store user information, ensuring strong privacy protections.

To improve service delivery, the government integrated ten commonly used public services into a single Government-to-Citizen (G2C) platform, streamlining access to services such as birth registration, marriage certificates, passports, license renewals, social security, and pensions. The Government Initiated Network (GIN) project further strengthened infrastructure by connecting 1,578 government institutions, including schools and hospitals, to a high-speed 10 Gbps network known as DrukREN. This has improved data sharing and collaboration across sectors.

Despite this significant progress, some issues remained. Limited coordination among relevant agencies slowed the implementation of certain projects. To address this, the Department of Information Technology and Telecom was proposed as the central coordinating body, responsible for facilitating implementation and appointing IT professionals across agencies. Additional obstacles included infrastructure constraints and the remoteness of rural areas. Projects such as the Electronic Patient Information System and the Bhutan Integrated Taxation System also experienced delays due to implementation and system upgrade needs. Development efforts continue to advance these initiatives to completion.

Educating consumers on safe digital practices and current cybersecurity protocols can significantly reduce the risks associated with digital financial transactions. Increasing awareness not only lowers losses and builds trust, but also empowers users to contribute to a more secure and resilient digital financial ecosystem.

A combined focus on robust digital identity systems, targeted outreach, and investment in digital literacy can support seamless and inclusive onboarding, while expanding connectivity and modernizing digital platforms are key to overcoming current limitations and increasing system capacity. By upgrading verification technologies, streamlining regulatory compliance, and reaching underserved areas, the region can build a secure, efficient digital ecosystem that benefits all citizens.

Strategic investments in infrastructure, unified data management, and inclusive technologies such as USSD-based services can reshape the digital financial landscape by driving economic growth, innovation, and equitable access to reliable digital services over the next three years. To ensure everyone can participate in this transformation, a public-private fund backed by governments and industry could be established to support nationwide digital literacy campaigns.

Ariadne Van Zandbergen / Alamy Stock Photo

5. MAJOR ACTION RECOMMENDATIONS: MEDIUM-TERM (THREE TO FIVE YEARS) – TOOLS FOR REGULATORS

Central to second-generation IDI is a set of strategies that build on first-generation FT4FI efforts to drive deeper financial inclusion and inclusive, sustainable development.

A. REGTECH AND SUPTECH: EMPOWERING AND EMPOWERED BY IDI

Leveraging technological tools for real-time compliance monitoring and risk management is a key opportunity to keep regulators agile and responsive in a rapidly evolving digital landscape. RegTech and SupTech, supported by second-generation IDI, plays a critical role in this evolution. Important applications include advanced fraud systems, digital regulatory reporting, and strengthening supervision through analytics and AI.

B. INVESTING IN AI-DRIVEN FRAUD DETECTION

Integrating artificial intelligence into fraud detection systems is critical. AI-powered analytics can continuously monitor transaction patterns, flag anomalies in real time, and identify potential threats before they escalate. This proactive approach minimizes financial losses while building consumer trust by reinforcing the security of DFS.

C. DIGITAL REGULATORY REPORTING AND REAL-TIME COMPLIANCE MONITORING

Digital Regulatory Reporting (DRR) seeks to transform financial data into digital formats that allow regulators to easily access and analyze information more efficiently, while maintaining appropriate controls.[65] DRR enables real-time risk monitoring, reduces the regulatory burden on Fis, and supports machine-readable and machine-executable regulations, allowing regulators to track updates, ensure compliance, and respond swiftly to emerging risks.[66] Data-driven solutions further this by automating regulatory change tracking, conducting stress tests, and improving adherence to evolving compliance requirements, all while reducing operational costs and enhancing regulatory agility.

D. SUPTECH FOR SUPERVISORY EFFICIENCY

Central banks and regulatory authorities are increasingly adopting SupTech tools to analyze large datasets, identify systemic risks, and streamline supervisory processes. AI-driven analytics and cloud-based regulatory dashboards enhance oversight capabilities, ensuring proactive risk mitigation. SupTech tools can assist regulators in extracting actionable insights from the collected data, monitor market surveillance via real-time alerts, and enforce penalties for market violations.[67] Additionally, SupTech applications can identify potential instances of money laundering, terrorism financing, fraudulent activities, and forecast mis-selling occurrences.[68] These capabilities support broader micro and macro-prudential regulatory goals, helping maintain market integrity, and safeguard consumers.[69]

E. LEVERAGING AI IN REGTECH AND SUPTECH TOOLS

When utilized responsibly, AI and machine learning can greatly improve the efficiency of RegTech-SupTech tools, improve business operations, reduce risks, and support more informed decision-making.[70] However, machine learning algorithms have inherent limitations and, if not properly monitored, can produce unreliable results. For example, a self-training model may generate biased outcomes if it is trained on skewed or biased data.[71]

65 Asian Development Bank. 2022. Building Regulatory and Supervisory Technology Ecosystems. Available at: https://www.adb.org/sites/default/files/publication/820686/regulatory-technology-ecosystems-asia-financial-stability.pdf

66 Id.
67 Id (at 29).
68 Id (at 28).
69 Id (at 30).
70 Id (at 34).
71 Id.

CASE STUDY: RBI's Mulehunter.ai

The Reserve Bank of India (RBI) has been proactive in addressing financial fraud, particularly in addressing the misuse of "mule" accounts (bank accounts used by criminals to launder illicit funds), often set up by unsuspecting individuals lured by promises of easy money or coerced into participating. The RBI Innovation Hub responded with the MuleHunter.ai[72] app to improve detection and reduce fraud.

MuleHunter.AI is designed to leverage advanced AI and machine learning algorithms to analyze transactions and account data to identify patterns indicative of mule accounts, significantly improving detection accuracy when compared to traditional rule-based systems. By drawing data from multiple sources, the app minimizes false positives that often burden static detection systems and enables near-real-time monitoring and faster detection of suspicious accounts. Its overarching goal is to protect the integrity of the financial ecosystem by curbing the spread of mule accounts.

Despite its benefits, the app has faced several challenges, including cybercriminals continuously adapting their tactics, making fraud detection increasingly complex. Integrating the app with the diverse IT infrastructures of different banks presents technical difficulties, and the resource- intensive nature of AI/ML systems demands significant investments in both skilled personnel and technological capacity.

Since its launch, MuleHunter.AI has achieved significant milestones, including successful pilots in two major public sector banks, which led to wider deployment. The app has demonstrated strong performance by significantly improving the detection of mule accounts and contributing to a reduction in financial fraud.

72 Further information is available at: https://rbihub.in/mule-hunter-ai/

Raushan_films / Shutterstock

6. MAJOR ACTION RECOMMENDATIONS: MEDIUM-TERM (THREE TO FIVE YEARS) – THE NEXT LEVEL OF IDI

As outlined in earlier sections, the region's progress in implementing FT4FI and IDI strategies has created new opportunities and emerging needs for second-generation approaches.

A. ADDRESSING DIGITAL FRAUD AND CRIME

While digital financial inclusion has seen notable success across the region and globally, it has inadvertently enabled the spread of digital fraud and crime, often placing the most vulnerable at highest risk. First-generation IDI systems can serve as the foundation for more advanced second-generation frameworks.

I. CENTRALIZED FRAUD REPORTING PORTALS

A unified fraud reporting portal, operated by a central authority, can act as a single point of contact for consumers nationwide. This portal could facilitate real-time aggregation and analysis of fraud data, allowing information to be shared more rapidly among regulators, FIs, and law enforcement agencies, and help identify emerging fraud patterns, enabling proactive measures to prevent future incidents.

Relevant examples include India's Citizen Financial Cyber Fraud Reporting and Management System, which links 85 banks, wallets, and payment intermediaries with a cybercrime backend portal. Users can report incidents to a phone helpline and receive a tracking ticket once registered. The portal facilitates coordination between police, banks, and payment platforms ensuring an efficient response.[73] Malaysia's National Fraud Portal, a partnership involving BNM and PayNet, automates scam report handling and fund tracing. It strengthens the effectiveness of the National Scam Response Centre by enabling automated fund tracing and recovery, preventing unauthorized transfers or withdrawals, facilitating industry-wide collaboration, and supporting data-driven analysis of mule accounts.[74]

73 Further information is available at: https://i4c.mha.gov.in/ncrp.aspx

74 Bank Negara Malaysia. 2024. National Fraud Portal to solidify coordinated efforts in curbing financial scams. Available at: https://www.bnm.gov.my/-/nfp-launch

II. DEVELOPING METRICS AND RESPONSE THRESHOLDS

A comprehensive cybersecurity framework should include clearly defined metrics to measure the impact of cyberattacks, such as the frequency and financial scale of fraud incidents. Establishing monetary thresholds and response timelines allows for swift, proportionate action when suspicious activities are detected. This data-driven approach not only improves responsiveness but can also effectively guide future policy and investment decisions.

III. TOOLS FOR MONITORING CONSUMER PROTECTION AND TRUST

Sustained growth and widespread adoption of digital finance depend heavily on maintaining consumer protection and trust. As DFS expands and cross-border interactions increase, protecting users from fraud, unfair practices, and data breaches is a non-negotiable responsibility. Without trust, adoption of digital financial tools can falter and lose ground. Regulators should, therefore, adopt benchmarks to monitor complaint resolution times, fraud incidence rates, and consumer satisfaction levels.

Tracking how quickly and effectively complaints are addressed offers insights into the responsiveness of consumer support systems. Monitoring fraud rates helps assess the security of digital financial systems, while customer satisfaction surveys provide direct feedback on user confidence. These indicators help regulators and industry stakeholders assess the effectiveness of protection measures and adjust policies as needed. Ongoing monitoring allows authorities to identify emerging risks and vulnerabilities, refine regulatory frameworks, and implement targeted interventions to strengthen consumer protection and maintain the integrity of the digital financial ecosystem.

B. TOOLS FOR ASSESSING FINANCIAL LITERACY INITIATIVES

Although central banks have long treated financial literacy as foundational to digital finance and launched initiatives across population segments, tools to measure the impact of these campaigns are still needed. This includes evaluating the return on investment in terms of time, funding, and resources spent by both regulators and their partners, along with tools such as VOC feedback to assess satisfaction, experience, and consumer perception. Regulators could leverage forums like SARFII to adopt locally tailored tools and benchmark their service quality. For instance, the Central Bank of Sri Lanka conducts periodic consumer surveys following its digital literacy campaigns to assess user proficiency and track changes over time.[75]

75 As noted by the Central Bank of Sri Lanka.

C. DIGITAL IDENTITY

Progress on foundational IDI has been substantial, but opportunities remain to deepen and fortify these systems.

I. ADOPTION OF ROBUST DIGITAL ID SOLUTIONS

To unlock the full potential of digital financial inclusion, consumers must be able access banking and FinTech services securely and with ease. Over the next three years, efforts should focus on building comprehensive digital identity systems to streamline the onboarding process and extending outreach to rural and underserved populations.

Digitizing national IDs and scaling up the adoption of digital ID systems with advanced biometric and facial recognition features is a key recommendation. Financial institutions can integrate these digital IDs into centralized e-KYC repositories to enable secure, frictionless account opening. Shared KYC systems across financial and non-financial sectors can support wider adoption, improve onboarding efficiency, and reduce fraud by ensuring consistent identity verification. This should be complemented by coordination with telecom authorities to align digital ID onboarding standards across sectors.

II. MANDATING DEVICE BINDING

Regulators should consider mandating mobile device binding for financial services to prevent unauthorized access and enable better tracking and blocking of illegal transactions.

CASE STUDY: Bangladesh National Digital Architecture (BNDA)

The flagship Bangladesh National Digital Architecture (BNDA) initiative was designed to improve digital governance, streamline service delivery, and ensure interoperability across government institutions. Developed by the Bangladesh Computer Council (BCC), BNDA aligns with international standards to ensure seamless data exchange, system interoperability, and improved public service efficiency.

Key components include the National e-Service Bus (NESB), which enables efficient integration of digital services across government agencies and supports Government-to-Government (G2G) data sharing, Government-to-Citizen (G2C) service delivery, Government-to-Business (G2B) collaboration, and Government-to-Employee (G2E) interactions, while also facilitating secure and reusable e-services that reduce redundancy and improve delivery efficiency. The e-Government interoperability framework ensures standardized communication between different government institutions, helping reduce duplication, improve cybersecurity, and raise data protection standards. These systems are integrated with a mobile service delivery platform that offers secure access to government services via mobile apps, integrated with digital ID and e-KYC verification.

Challenges remain for BNDA despite this success. Limited digital literacy and relatively high rural internet costs hinder widespread adoption, while both financial institutions and government agencies require additional support to achieve full integration. Strengthening data security will also be important to align with international data protection standards.

Martin Bertrand / Alamy Stock Photo

D. CONSUMER PROTECTION

As digital financial services expand, establishing robust consumer protection mechanisms becomes increasingly critical to build and sustain trust in the digital ecosystem. Over the next three years, efforts should focus on developing comprehensive regulatory frameworks that safeguard consumers while promoting transparency, accountability, and swift dispute resolution. Special attention is needed for vulnerable groups often excluded from the digital transition, with inclusive policies addressing gender gaps, age-related challenges, and socioeconomic disparities to ensure equitable access. An effective consumer protection strategy requires coordination across regulatory frameworks, clear accountability for fraud, and enhanced consumer education. Together, these measures can strengthen trust and participation in digital finance, creating an environment for greater adoption and sustainable growth while safeguarding consumer interests.

I. COMPREHENSIVE CONSUMER PROTECTION REGULATIONS

A primary recommendation is to finalize and implement unified consumer protection regulations that cut across various financial services. These should be in line with efforts to integrate fragmented complaint and redress systems into a centralized framework, ideally managed by a national authority or central bank, through which consumers will have a clear and accessible path to resolve disputes. Regulators should adopt a proportionate, consolidated approach when full unification is limited by legal or structural challenges, helping streamline processes, reduce resolution times, and ensure consistent handling of consumer grievances across different sectors.

II. ENHANCED DISCLOSURES AND REDRESS MECHANISMS

Mandating clear and standardized disclosures on fees, transaction terms, and data privacy will help consumers make informed choices and build confidence in digital transactions. Additionally, robust redress mechanisms should also be established, with defined timelines for resolving complaints. This should include clear protocols for temporary measures, such as freezing suspect accounts during fraud investigations, to protect consumers while maintaining the integrity of the financial system.

E. CYBERSECURITY AND DATA PROTECTION

As DFS grows, strengthening cybersecurity and data protection is critical to safeguard both consumers and financial institutions from evolving digital threats. Over the next three years, strategic investments in advanced threat detection, rapid incident response, and inter-agency coordination will be essential to maintaining a resilient digital ecosystem. This must include prioritizing research and development to anticipate and counter emerging risks from technologies such as deep fakes, synthetic identities, and AI-powered scams.

To reinforce security, multi-factor authentication should be widely implemented as part of a layered approach that includes biometric verification, one-time passwords, and contextual security checks, measures which can help secure user access even if credentials are compromised. Protecting sensitive financial data and preventing unauthorized access also requires strong data storage and sharing policies, backed by strict penalties that go beyond fines to include operational restrictions for severe violations.

To address rising cybersecurity threats, regulators should mandate timely breach notifications, compelling organizations to promptly report incidents. In India, the Digital Personal Data Protection Act (2023) imposes strict penalties for non-compliance, including fines of up to INR250 crore (approximately USD30 million).[76] Proactive risk management strategies, such as regular audits and security assessments, should also be required to prevent potential data leaks and cyberattacks.

A coordinated approach is the key to success. This includes unifying fragmented consumer complaint mechanisms into a single, accessible platform, ideally overseen by a central authority such as the central bank. Such integration would facilitate comprehensive tracking of fraud, enable streamlined dispute resolution, and help improve regulatory responses.

F. REGULATORY FRAMEWORKS

To sustain a secure and dynamic digital finance ecosystem, the next three years should focus on legal and regulatory frameworks that promote innovation while ensuring consumer protection and market stability. This requires a cohesive strategy to modernize outdated laws, harmonize fragmented policies, strengthen oversight, and build regulatory capacity. Progress can be accelerated through improved inter-agency coordination and by establishing dedicated councils to ensure reforms remain responsive to technological advancements.

76 Further information is available at: https://www.dlapiperdataprotection.com/?t=breach-notification&c=IN

G. DATA PRIVACY REGULATIONS AND FRAMEWORKS

Given the rapid digitalization taking place across sectors, regulators should implement sector-specific data privacy guidelines tailored to industries such as financial services, healthcare, and e-commerce. FinTech firms, for instance, must follow stringent cybersecurity and fraud prevention protocols. Sri Lanka's Personal Data Protection Act[77] includes provisions that protect financial and healthcare data, ensuring confidentiality in medical records and when using research data,[78] while Nepal's Digital Lending Guidelines require FIs and PSPs to protect borrower information and ensure strict confidentiality.[79]

Strong enforcement mechanisms are critical for effective data privacy, yet many SAFRII members face resource constraints. Investments in RegTech, independent data protection authorities, and cross-agency collaboration are needed to better support compliance, while building regulatory capacity can further improve oversight and enforcement.

A core element of data privacy is giving individuals control over their personal data. Regulators should mandate clear, informed, and revocable consent mechanisms so users understand and manage how their data is collected, processed, and shared. Defining data ownership rights in the context of AI-driven decision-making, automated profiling, and digital identity frameworks will also be crucial in addressing emerging privacy concerns. Pakistan's proposed Personal Data Protection Bill supports user empowerment by mandating explicit consent and withdrawal rights.

Data privacy regulations are only effective when individuals understand their rights and responsibilities. Governments should expand digital literacy programs to raise awareness of data protection, consent, and cybersecurity best practices. India's Cyber Surakshit Bharat initiative, for instance, promotes cybersecurity education among citizens and businesses, while similar efforts in Bangladesh and Sri Lanka are focused on increasing consumer awareness and responsible data usage.

77 Further information is available at: https://www.parliament.lk/uploads/acts/gbills/english/6242.pdf

78 Graham Greenleaf. 2022. Sri Lanka's Personal Data Protection Act is Finalised with a Stronger DPA. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4181012#:~:text=Abstract.%20Sri%20Lanka's%20Personal%20Data%20Protection%20Act,is%20arguably%20independent%2C%20and%20with%20broad%20powers

79 Pradhan & Associates. 2022. NRB's Guideline on Digital Lending. Available at: https://pradhanlaw.com/file-upload/files/NRB%E2%80%99sGui-1681804515.pdf

Rupixen / Unsplash

H. FEE STRUCTURE REFORMS

Cost remains a substantial barrier to digital adoption for small merchants and low-income users. Merchant Discount Rates (MDRs) vary by country, ranging from zero fees for specific transactions to uncapped MDRs set by providers. In some cases, governments subsidize some fees to encourage digital payments. On the other hand, credit card MDRs can reach up to 3.5 percent in some markets, with merchants also bearing the cost of PoS devices. For mobile payments, especially Person-to-Person (P2P) and Person-to-Merchant (P2M), low margins make it difficult for providers to remain viable under zero or minimal fee structures, especially if they are limited to payments without offering other financial services.

Implementing fee structure reforms, such as standardized MDRs and tiered fees for instant payment systems based on transaction size and merchant volume, can improve affordability and sustainability for consumers. For example, transactions below a 5,000 local currency threshold might remain fee-free, while higher value payments could attract graduated fees. This structure encourages broader participation while ensuring higher value transactions and larger merchants contributing fairly to the ecosystem's maintenance. SARFII members could establish a taskforce to evaluate the effectiveness and modalities of a balanced payment fee structure that supports payment operators, and consumers and merchants.

To further incentivize payment operators, regulators might consider fast-tracking additional licenses for financial services such as lending. Extensions should be merit-based, reflecting the level of activity (transaction volumes, user numbers, etc.), and a strong compliance track record under the primary license, while maintaining robust prudential requirements.

Egon Boemsch / Alamy Stock Photo

I. LIABILITY MANAGEMENT

To effectively counter rising fraud and cybercrime while protecting customers who are not at fault, developing and implementing detailed fraud liability frameworks must be a top priority. These should specify the responsibilities of FIs and consumers, outline the process for determining liability, and set clear thresholds for initiating fraud investigations. Timebound response requirements for licensed institutions can further help expedite incident resolution by defining each stakeholder's role and responsibilities.

Another consideration is developing insurance frameworks for digital financial fraud, modeled on global best practices for credit card fraud. This will require collaboration between banking and insurance regulators to design viable policies while encouraging insurance companies to offer products that protect both institutions and consumers.

J. DIGITAL LENDING FRAMEWORKS

While payments are a key component of DFS, access to credit remains a foundational need, especially in lower income markets. Affordable and easy to access credit can empower individuals and SMEs, accelerating their financial progress. Digital lending expands this access, including for those excluded from formal channels due to limited credit history. By leveraging alternative data and AI-driven models, digital lenders can more effectively offer loans to underserved segments. However, while traditional banks and credit institutions operate under established regulations, the regulatory framework for digital lending, especially standalone digital credit providers, is still evolving in the region.

An effective digital lending framework should address the following key elements:

I. LOAN DISPENSATION PROCESS

Borrowers must be clearly informed of interest rates, fees, and repayment terms to ensure transparency. Regulators may also consider introducing a cooling-off period, based on loan size. Depending on the existing structure of the market, loans should ideally be disbursed directly to the borrower's bank account rather than through intermediaries, which can introduce additional complexities and risks.

- **I.A. ASSESSING CREDITWORTHINESS**

  The frameworks should allow the use of credit scoring models that leverage alternative data sources, such as utility payments and social media activity, to assess creditworthiness, especially for individuals without traditional credit histories. AI-driven models can further enhance the accuracy and speed of these assessments, provided governance frameworks are in place that ensure fairness and removal of bias.

- **I.B. DIGITAL LENDING LIMITS AND MATURITY PERIODS**

  Digital lending can support borrowers with urgent credit needs, but establishing clear limits and caps on loan amounts and maturity periods helps prevent over-indebtedness while still balancing short-term credit needs.

- **I.C. DATA PROTECTION**

  Regulators should implement robust consent-based data protection rules to safeguard personal and financial information, covering encryption, secure storage of sensitive data, and setting data retention limits for lenders. These measures should align with existing data protection laws, where applicable, with regular audits reinforcing sound data governance practices.

- **I.D. FRAMEWORKS FOR BALANCE SHEET-BASED LENDING AND TECH PLATFORMS**

  The frameworks should cover both balance sheet lending terms and detailed rules for FinTechs and digital platforms that originate and process loans through partners without lending from their own balance sheets.

K. OPEN BANKING AND OPEN FINANCE

Open Banking frameworks allow authorized third-party providers to access customer data and initiate payments with customer consent, encouraging innovation and competition through standardized APIs that enable seamless communication and data exchange among FIs and payment systems. This integration facilitates real-time, cross-border transactions, reduces dependence on correspondent banking networks, and lowers transaction fees. Mandating open APIs and standardized interfaces promotes platform integration while allowing non-financial institutions such as e-commerce, asset management, and utilities to seamlessly connect with traditional financial services, thereby dismantling operational silos and supporting a unified digital payments experience for both consumers and merchants.

As regulators in the region enhance IDI policies, consolidating existing frameworks into unified digital finance regulations, integrating FinTech, data protection, and cybersecurity, would be highly beneficial simplifying compliance, supporting innovation, and ensuring consistent consumer protection standards across the region. Given the rapidly-evolving nature of digital finance, regulatory frameworks must remain agile through built-in review mechanisms and adaptive clauses that allow periodic updates to respond to technological change and market developments, enabling a balance between risk mitigation and innovation.

Regulatory interventions should also be proportionate to the scale, risk, and complexity of financial activities and entities, as overly burdensome requirements on small FinTechs or micro-enterprise solutions can impede financial inclusion and product development. A formal and ongoing consultative forum involving regulators, industry participants (including new market entrants), consumer groups, tech innovators, and academic experts would create a space for open dialogue, shared understanding of emerging technologies and risks, and the co-creation of practical, effective, and future-ready regulatory approaches.

The success of DFS depends on coordinating infrastructure integration with forward-thinking regulatory practices, aligning strategic roadmaps with measurable KPIs, incentivizing collaborative ecosystems, and ensuring that fee structures advance inclusive growth across all market segments. Although mobile infrastructure and connectivity fall outside the central bank's direct mandate, they are critical for the delivery of DFS in remote areas and among mobile-only users. Central banks should, therefore, coordinate with telecom authorities and IT ministries to extend coverage, while tracking metrics such as network uptime, broadband speed, and last-mile connectivity to assess the system's readiness for advanced digital finance.

7. BUILDING A REGIONAL CROSS-BORDER STRATEGY

In addition to assessing each country's status and strategic priorities, as outlined in the previous section, there are broader regional opportunities grounded in ongoing or proposed SARFII initiatives.

As digital financial ecosystems mature, advancing cross-border integration and defining clear benchmarks will lay the groundwork for a more cohesive and competitive regional market. Closer collaboration among member countries will strengthen capacity, unlock shared resources, and support deeper peer learning and knowledge exchange. AFI and SARFII can play a catalytic role in making these efforts more effective. Over the next three to five years, regional stakeholders must prioritize strategies that enable interoperability between national systems, while setting measurable targets to track progress and ensure continuous improvement.

A. HARMONIZING REGULATORY FRAMEWORKS AND ENHANCING COLLABORATION

Developing unified legal and regulatory standards that extend beyond national boundaries is essential for enabling seamless cross-border transactions and regional collaboration. Varying regulations across jurisdictions, such as digital payment protocols, cybersecurity standards, and consumer protection measures, often create operational complexity undermining the smooth delivery of DFS across borders. Differences in KYC verification procedures or data privacy standards, for example, can pose challenges for FIs and FinTechs operating regionally.

To reduce these barriers, regulators must work toward harmonizing frameworks, particularly in areas such as digital public infrastructure, credit information systems, and shared utility platforms for tracking fraud and scams. Establishing consistency in these areas will help create a more predictable, transparent environment that supports innovation and streamlines compliance for firms operating across multiple markets. Collaborative tools such as shared innovation hubs or cross-border regulatory sandboxes can accelerate the development of new technologies and financial products by enabling regulators and innovators from different countries to jointly test new solutions and share knowledge in a controlled setting. This harmonized approach can simplify compliance, encourage investment, reduce transaction costs, and improve processing times, while also expanding DFS across the region. Ultimately, this will support the deeper integration of South Asian markets and contribute to sustainable economic growth.

B. INTEGRATING PAYMENT SYSTEMS AND DATA

Establishing interoperable digital payment networks across the region is a strategic priority for enabling real-time, cost-effective transactions. Many national systems currently operate in isolation, limiting the ability of individuals and businesses to transact seamlessly across borders and restricting the potential of regional trade, remittances, and e-commerce. By promoting open banking initiatives and standardized APIs, FIs can improve transaction efficiency, reduce costs, and access to DFS for consumers and businesses.

South China Morning Post / Alamy Stock Photo

Bilateral FinTech and payment initiatives among SARFII members have shown promise, particularly in partnerships involving India. While notable remittance flows such as those from the Maldives to Bangladesh exist, most significant cross-border activity remains limited and often involves non-SARFII members. To address this, members could explore the development of a multi-country interoperability platform, similar to Southeast Asia's Project Nexus,[80] potentially linked with the SAARC payment initiative, to connect domestic instant payment systems across the region.

Such interoperable systems can make cross-border financial services more accessible and affordable, especially for underserved populations and SMEs, enabling broader participation in regional economic activity. Supporting this integration requires a parallel focus on secure data exchange. Regional data-sharing protocols with strong privacy and security safeguards can enhance fraud detection, risk management, and regulatory oversight by enabling more effective monitoring of financial flows and criminal activity that crosses national boundaries. With a more holistic view of regional financial risks and activities, regulators will be better positioned to shape responsive and forward-looking policies.

C. DEFINING MEASURABLE TARGETS FOR CROSS-BORDER INITIATIVES

To effectively track progress in cross-border digital finance integration and maintain accountability, clear and measurable benchmarks must be established in alignment with the core objectives of regional interoperability. Not having specific targets makes it difficult to evaluate the impact of implemented strategies or identify areas requiring further intervention. These KPIs should encompass dimensions such as the volume and frequency of cross-border transactions, adoption rates of interoperable payment platforms, and improvements in cybersecurity resilience across systems. Establishing such quantitative targets will provide a clear roadmap for achieving a more integrated and inclusive digital finance ecosystem. In parallel, member countries can contribute by sharing locally developed tools used for regulatory impact assessments and policy evaluations. These efforts can be complemented through AFI working groups, which could lead the development of a regional framework of best-practice guidelines for monitoring initiatives such as consumer protection campaigns, digital literacy programs, and broader financial inclusion policies.

80 Monetary Authority of Singapore. 2024. Project Nexus completes comprehensive blueprint for connecting domestic instant payment systems globally and prepares for work towards live implementation. Available at: https://www.mas.gov.sg/news/media-releases/2024/project-nexus-completes-comprehensive-blueprint-for-connecting-domestic-ipses-globally

8. CONCLUSION

The project has identified substantial progress across SARFII in advancing financial inclusion and inclusive sustainable development through first-generation FT4FI and IDI strategies implemented over the past decade. Despite the meaningful gains so far, ongoing challenges remain, including enduring digital divides, evolving cyber risks, uneven regulatory capacity, and limited interoperability across markets. Additionally, new concerns have emerged from the success of digital inclusion, such as increased vulnerability to digital fraud and the complexities of regulating more sophisticated DFS.

This report detailed the successes as well as the road ahead, underscoring the value of first-generation FT4FI and IDI strategies while synthesizing a range of lessons from implementation across the region. These insights are not only relevant to SARFII members but also offer important reference points for other AFI members undertaking similar transitions in their digital finance and infrastructure.

Looking ahead, the progress to date opens new opportunities for second-generation IDI strategies, building on existing systems to deepen their impact and effectiveness. Areas such as digital fraud mitigation, regulatory reporting, and the development of data and lending infrastructures are emerging as critical pillars of next generation IDI, offering fresh avenues for innovation and inclusion. By continuing to take up this challenge, SARFII members can lead by example, shaping approaches that not only serve their own populations but also inspire and guide efforts across the broader AFI network.

Aleksandr Davydov / Alamy Stock Photo

BIBLIOGRAPHY

BANGLADESH

- Alliance for Financial Inclusion. 2022. Bangladesh's 2021–2026 National Financial Inclusion Strategy Overview. Available at: https://www.afi-global.org/publication/bangladeshs-2021-2026-national-financial-inclusion-strategy/
- Bangladesh Bank. 2023. Bangladesh Financial Inclusion Report 2023. Available at: https://www.bb.org.bd/pub/annual/finreport/finreport_2023.pdf
- Bangladesh Bank and the University of Dhaka. 2017. An Impact Study on Mobile Financial Services (MFS) in Bangladesh. Available at: https://www.bb.org.bd/pub/special/impact_mfs_27092018.pdf
- Bangladesh Cyber Security Strategy 2021–2025. n.d. Framework outlining national goals for cyber resilience and digital security. Available at: https://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/page/6c9773a2_7556_4395_bbec_f132b9d819f0/nothi_10314_2021_07_30_31627641428.pdf
- CIRT - Cybersecurity Strategy Responsibility Matrix. 2022. Detailed allocation of responsibilities for implementing the cybersecurity strategy. Available at: https://www.cirt.gov.bd/meeting-on-bangladesh-cybersecurity-strategy-2021-2025-responsibility-matrix/
- Financial Literacy Guidelines. 2022. Regulatory guideline outlining approaches to improving financial literacy across Bangladesh. Available at: https://www.bb.org.bd/mediaroom/circulars/finincld/mar272022fid01.pdf
- Gender-Centric Financial & Digital Literacy Assessment – a2i. 2023. Study exploring gender disparities in digital financial access and skills. Available at: https://a2i.gov.bd/wp-content/uploads/2023/11/1.2-Gender-Centric-Financial-Digital-Literacy-Assessment-1.pdf
- National Financial Inclusion Strategy (NFIS) 2021–2026. n.d. Bangladesh Bank's official strategy document for universal financial inclusion. Available at: https://www.bb.org.bd/aboutus/regulationguideline/nfis_eng.pdf
- Survey on ICT Use and Access by Individuals and Households 2022. 2022. A national statistical report on mobile, internet access, and digital divide issues. Available at: https://bbs.portal.gov.bd/sites/default/files/files/bbs.portal.gov.bd/page/b343a8b4_956b_45ca_872f_4cf9b2f1a6e0/2023-01-08-07-00-667cde6536494c707e86d483c0b618a5.pdf

BHUTAN

- Credit Information Bureau of Bhutan. n.d. Available at: https://www.cib.bt/CIB/about.php
- ncino. n.d. Small Business Loan Origination System. Available at: https://www.ncino.com/en-US/solutions/small-business-loan-origination-system
- Royal Monetary Authority of Bhutan. 2022. Rules and Regulation on Loan Origination and Monitoring 2022. Available at: https://www.rma.org.bt/media/Laws_By_Laws/Rules%20and%20regulation%20on%20Loan%20origination%20and%20monitoring%202022.pdf
- Royal Monetary Authority of Bhutan. 2019. Cybersecurity Directives for Banks. Available at: https://www.rma.org.bt/media/Laws_By_Laws/%20Cybersecurity%20Directives%20for%20Banks.pdf
- Royal Monetary Authority of Bhutan. n.d. Payment Systems: An overview of Bhutan's payment systems and initiatives undertaken by the Royal Monetary Authority to promote digital payments. Available at: https://www.rma.org.bt/publication/24/
- Royal Monetary Authority of Bhutan. n.d. Financial Consumer Protection Survey Report. Available at: https://www.rma.org.bt/bank/RMA%20Publication/papers/Financial%20Consumer%20Protection%20Survey%20Report.pdf
- The Bhutanese. n.d. Bhutan launches QR code payment system. Available at: https://www.rma.org.bt/dpSystem/

NEPAL

- NEPALPAY QR. n.d. Nepal Clearing House Limited. Available at: https://nchl.com.np/nepalpay-qr/
- Nepal Payment Systems Development Strategy. 2019. Available at: https://www.nrb.org.np/contents/uploads/2019/12/Nepal-Payment-Systems-Development-Strategy.pdf

- Nepal Rastra Bank Consumer Protection Portal. n.d. Available at: https://www.nrb.org.np/departments/ficpd/
- Nepal Rastra Bank. 2020. QR Code Guidelines and Framework 2021. Available at: https://www.nrb.org.np/contents/uploads/2021/01/QR-Code-Guidelines-and-Framework-and-Specifications.pdf
- Nepal Rastra Bank. 2019. Retail Payment Strategy 2019. Available at: https://www.nrb.org.np/contents/uploads/2019/12/Retail-Payment-Strategy-2019.pdf
- National ID (NID) Program – Nepal. n.d. Available at: https://nid.npc.gov.np/
- connectIPS by Nepal Clearing House. n.d. Available at: https://www.connectips.com/
- World Bank. n.d. Nepal Digital Financial Services Initiatives – Supports NRB in strategy, inclusion, and cyber resilience. Available at: https://www.ifc.org/content/dam/ifc/doc/2025/digital-financial-services-in-nepal.pdf

THE MALDIVES

- eFaas. n.d. The Maldives' National Digital Identity. Available at: https://efaas.egov.mv/
- FahiPay. n.d. The Maldives' Mobile Payment Solution. Available at: https://techmaldives.com/fahipay-maldives-mobile-payment-solution
- Maldives Monetary Authority. n.d. Payment Systems (overview of the payment systems, including efforts to modernize and promote digital transactions). Available at: https://mma.gov.mv/payment-systems
- Maldives Monetary Authority. 2023. Guideline on Incident Reporting for Payment Service Providers. Available at: https://www.mma.gov.mv/documents/Payments%20Infrastructure/Guideline%20on%20Incident%20Reporting%20for%20Payment%20Service%20Providers.pdf
- Maldives Monetary Authority. 2022. National Financial Inclusion Survey 2022. Available at: https://www.mma.gov.mv/documents/National%20Financial%20Inclusion%20Survey/2022/NFI-Survey-2022.pdf
- World Bank. 2024. Maldives Financial Sector Assessment Program - Technical Note. Available at: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099060624144515101/p18010018ba7020fc1bd1b12ee8ea7e80dc

PAKISTAN

- State Bank of Pakistan. 2024. Annual Payment Systems Review. Available at: https://www.sbp.org.pk/press/2024/Pr-11-Oct-2024.pdf
- Mettis Global News. 2024. Digital Payments Surge 35% in FY24. Available at: https://mettisglobal.news/pakistans-digital-payments-surge-35-in-fy24/
- State Bank of Pakistan. 2024. Payment Systems Annual Review 2023-24. Available at: https://www.sbp.org.pk/PS/PDF/FiscalYear-2023-24.pdf
- State Bank of Pakistan. n.d. Branchless Banking Statistics for Jul-Sep 2024. Source for data on BB accounts (122.9M), agents (693K+), and daily transactions. Available at: https://www.sbp.org.pk/acd/branchless/Stats/Branchless%20Banking%20Statistics%20for%20Jul%20-%20Sep%202024.pdf
- State Bank of Pakistan. n.d. Payment Systems Quarterly Review Q1 FY25. Available at: https://www.sbp.org.pk/psd/pdf/PS-Review-Q4FY25.pdf
- State Bank of Pakistan. Digitalization to drive Financial Services and Economic Development: Governor SBP. Available at: https://www.sbp.org.pk/press/2024/Pr-02-Oct-2024.pdf
- Karandaaz Pakistan. n.d. Banking Infrastructure and Transactions. Available at: https://portal.karandaaz.com.pk/category/banking-infrastructure-and-transactions/2002
- Data Darbar Insights. 2024. Financial Inclusion from a Provincial Lens. Available at: https://insights.datadarbar.io/financial-inclusion-from-a-provincial-lens

SRI LANKA

- Information and Communication Technology Agency (ICTA) of Sri Lanka. n.d. Digital Identity in Sri Lanka – SL-UDI Project. Available at: https://www.icta.lk/projects/digital-government/sludi
- Central Bank of Sri Lanka. n.d. A Guide to Payment Services in Sri Lanka. Available at: https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/publications/guide_to_payment_services_in_sl.pdf

- Central Bank of Sri Lanka. n.d. Payments and Settlements Systems. Available at: https://www.cbsl.gov.lk/en/financial-system/financial-infrastructure/payments-and-settlements-systems
- Central Bank of Sri Lanka. n.d. Digital Payments Promotion Campaign 2025. Available at: www.cbsl.gov.lk/en/news/digital-payments-promotion-campaign-2025
- Central Bank of Sri Lanka. n.d. Consumer Protection Framework Enforced February 2024. Available at: www.cbsl.gov.lk/en/news/consumer-protection-framework-enforced-february-2024
- Central Bank of Sri Lanka. n.d. FinTech Regulatory Sandbox. Available at: https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/about/20200214-FinTech-Regulatory-Sandbox-of-CBSL-Framework-e.pdf
- Central Bank of Sri Lanka. 2025. Fast Payments for Everyone — CEFTS Implementation in Sri Lanka. Available at: https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/statistics/otherpub/information_series_note_20250224_fast_payments_for_everyone_cefts_implementation_in_srilanka_e.pdf
- Central Bank of Sri Lanka. 2025. Central Bank of Sri Lanka Launches the Digital Payments Promotion Campaign 2025. Available at: https://www.cbsl.gov.lk/en/news/cbsl-launches-the-digital-payments-promotion-campaign-2025
- Department of Census and Statistics. 2021. Digital Literacy Gap in Sri Lanka (Urban-Rural-Estate Sector). 2021. Available at: www.statistics.gov.lk/education/ICT_Use_2021
- FinCSIRT. n.d. Sri Lanka's Cybersecurity Coordination Body. Available at: www.fincsirt.lk/
- Lanka Pay (previously Lanka Clear). n.d. LANKAQR and JustPay in Sri Lanka's Fast Payment System. Available at: https://www.lankapay.net/en/for-you/justpay
- Ministry of Science and Technology. 2022. Personal Data Protection Act, No. 9 of 2022. Available at: https://www.parliament.lk/uploads/acts/gbills/english/6242.pdf

ACRONYMS

2FA	Two-Factor Authentication
AA	Account Aggregator - India
AFI	Alliance for Financial Inclusion
AI	Artificial Intelligence
AMA	Asaan Mobile Accounts - Pakistan
AML	Anti-Money Laundering
API	Application Programming Interface
BB	Branchless Banking
BCC	Bangladesh Computer Council
BITS	Bhutan Integrated Taxation System
BNDA	Bangladesh National Digital Architecture
CAPEX	Capital Expenditure
CBDC	Central Bank Digital Currency
CBSL	Central Bank of Sri Lanka
CEFTS	Common Electronic Fund Transfer Switch - Sri Lanka
CIB	Credit Information Bureau - Bhutan
CIRT	Computer Incident Response Team
CISO	Chief Information Security Officer
CNIC	Computerized National Identity Card - Pakistan
FT4FI	AFI FinTech for Financial Inclusion Strategy
FTC	Fair Treatment of Customers framework - Pakistan
DFS	Digital Financial Services
DITT	Department of Information Technology and Telecom - Bhutan
DPI	Digital Payment Infrastructure
DRR	Digital Regulatory Reporting
EGovPayment	Electronic Government Payments
e-KYC	Electronic Know Your Customer
FAST	FinTech and Startup Acceleration - India
FI	Financial Institution
FinCSIRT	Financial Sector Computer Security Incident Response Team - Sri Lanka
FPS	Fast Payment System
FT4FI	FinTech for Financial Inclusion - AFI's 2018 strategy for technology-driven financial inclusion
G2B	Government-to-Business
G2C	Government-to-Citizen
G2E	Government-to-Employee
G2P	Government-to-Person
GIN	Government Initiated Network - Bhutan
ICT	Information and Communication Technology
ICTA	Information and Communication Technology Agency - Sri Lanka
IDI	Inclusive Digital Infrastructure
IFC	International Finance Corporation - World Bank Group
IPS	Instant Payment System
ISO 27001	International Organization for Standardization 27001
IT	Information Technology

ITU	International Telecommunication Union
KPI	Key Performance Indicator
KYC	Know Your Customer
LFI	Licensed Financial Institution
MDR	Merchant Discount Rate
MFA	Multi-Factor Authentication
MFS	Mobile Financial Services
MMA	Maldives Monetary Authority
MSDP	Mobile Service Delivery Platform - Bangladesh
MSME	Micro, Small, and Medium Enterprises
NBFC	Non-Banking Finance Companies
NCIT	National Centre for Information Technology - Maldives
NDI	National Digital Identity - Bhutan
NESB	National e-Service Bus - Bangladesh.
NFIS	National Financial Inclusion Strategy
NIC	National Identity Card - Sri Lanka
NID	National Identification
NPCI	National Payments Corporation of India
NRB	Nepal Rastra Bank
OTP	One-Time Password
P2M	Person-to-Merchant
P2P	Person-to-Person
PIDF	Payments Infrastructure Development Fund - India
PoC	Proof of Concept
PoS	Point of Sale
PSPs	Payment Service Providers
PTA	Pakistan Telecommunication Authority
QR	Quick Response - Codes for digital payments
RBI	Reserve Bank of India
RBIH	Reserve Bank Innovation Hub
RMA	Royal Monetary Authority - Bhutan
SAARC	South Asian Association for Regional Cooperation
SARFII	South Asian Region Financial Inclusion Initiative - AFI
SBP	State Bank of Pakistan
SLPA	Sri Lanka Port Authority
SL-UDI	Sri Lanka Unique Digital Identity
SME	Small and Medium Enterprises
SRO	Self-Regulatory Organization
SRO-FT	Self-Regulatory Organization for FinTech
SupTech	Supervisory Technology
TMCO	Total Cost of Mobile Ownership
TRCSL	Telecommunications Regulatory Commission of Sri Lanka
UN ECC	United Nations Electronic Communications Convention
UPI	Unified Payments Interface - India
USSD	Unstructured Supplementary Service Data

ANNEX A
SURVEY QUESTIONS FOR A COMPREHENSIVE DIAGNOSTIC ASSESSMENT OF SARFII MEMBERS' DIGITAL ECOSYSTEMS

SECTION 1: DIGITAL FINANCIAL SERVICES

1. What are the main barriers to using digital financial services in your region? (e.g. lack of digital literacy, limited infrastructure, cost). Provide the reasons for why these barriers exist.

2. On a scale of 1 to 10, how accessible are digital financial services for people with low digital literacy?

3. How do gender or socioeconomic factors affect access to digital financial services in your community? Please provide examples.

4. Please provide examples of any hidden costs or fees associated with digital financial services that might disproportionately affect low-income users, or women?

5. What efforts are being made to overcome language and literacy barriers in digital financial services? These can include anything from education to other incentives.

SECTION 2: CONSUMER PROTECTION

1. On a scale of 1 to 10, how confident are you in the security of digital financial services? (1 being not confident, 10 being very confident)

2. What are the potential risks associated with using digital financial platforms? Please list them (e.g. fraud, data breaches).

3. On a scale of 1 to 10, how informed are users about their rights and responsibilities when using digital financial services?

4. On a scale from 1 to 10, do you believe users understand the terms and conditions of the services they use? (1 is they do not understand and 10 they fully understand)

5. Please provide examples of how financial service providers and FinTechs educate consumers effectively about safe practices (e.g. identifying phishing scams, secure password creation)?

6. How easy is it for users to have their rights vindicated if they sense there has been a violation? (Scale of 1-10, with 1 being really hard and 10 being really easy)

7. Please provide any recommendations or comments that can support the enhancement of consumer protection in the provision of digital financial services. Please also include specific recommendations on dispute resolution and complaint handling mechanisms.

SECTION 3: DATA GAPS, NEEDS, AND GOVERNANCE

1. How can financial institutions, technology providers, and governments collaborate to improve data management systems? Please provide any relevant examples.

2. What type of training or capacity-building programs do you think are needed for stakeholders involved in data management? Give the reasons why.

3. On a scale of 1 to 10, with 1 being insufficient and 10 being extremely sufficient, how sufficient are existing regulations in addressing the challenges in data management for digital financial services?

4. In reference to the previous question, why or why not (are the regulations sufficient)? Please also name any relevant regulations and explain their purpose.

5. Based on your knowledge, what type and approach of digital identity systems could ensure data reliability and accessibility?

6. What processes are in place for regularly auditing and monitoring data management practices in your organization or institution?

7. On a scale of 1 to 10, with 1 being least effective and 10 being most effective, how effective are independent bodies or mechanisms in ensuring accountability in data handling?

8. Please provide examples where data analytics are being utilized to identify underserved populations and create tailored financial products?

9. On a scale of 1 to 10, how effective are current data-sharing frameworks at ensuring seamless integration between financial institutions, FinTechs, and other stakeholders?

SECTION 4: SME FINANCE

1. What initiatives are in place to educate SMEs about the benefits and usage of digital financial platforms?

2. On a scale from 1 to 10, with 1 being not confident and 10 being very confident, how confident do SME owners feel about using digital platforms for financial transactions? Please also explain your perspective.

3. On a scale of 1 to 10, with 1 being not very accessible and 10 being very accessible, how reliable and accessible is the digital infrastructure (e.g. internet connectivity, mobile networks) for SMEs in your area?

4. What challenges do SMEs face in integrating digital financial tools with their existing business operations?

5. What recommendations would you provide to enhance SMEs' access to digital finance?

ANNEX B
LIST OF NON-SARFI MEMBER ORGANIZATIONS WHOSE INPUT WAS TAKEN DURING IN-COUNTRY VISITS (EXCLUDING SURVEY PARTICIPANTS):

Country	**Institution**
Nepal	Muktinath Bikas Bank Limited
	Nepal Clearing House Limited
	Nepal Payment Solution
	City Pay Pvt. Ltd.
	Machhapuchhre Bank Limited
	Nabil Bank Limited
	CityTech
	Fintech Alliance Nepal
Sri lanka	Lankapay (pvt) ltd
	People's Bank
	Hatton National Bank
	Nations Trust Bank
	LOLC Finance PLC
	Dialog Axiata PLC
	Mobitel (Pvt) Ltd
	Sri Lanka Financial Sector Computer Security Incident Response Team (FinCSIRT)
	PAYMEDIA/DIRECT PAY
India	Reserve Bank of India (RBI)
	National Payments Corporation of India (NPCI)
	Gates Foundation
	Sahamati
	Internet and Mobile Association of India (IAMAI)/Payments Convergence Council
	Digital Lending Association of India (DLAI)

Alliance for Financial Inclusion
AFI, Sasana Kijang, 2, Jalan Dato' Onn, 50480 Kuala Lumpur, Malaysia
t +60 3 2776 9000 **e** info@afi-global.org www.afi-global.org
Alliance for Financial Inclusion AFI.History @NewsAFI @afinetwork